Technical Guidance for College and University CIOs and CTOs in Complying with HEOA Provisions

(Revision 1)

CONTENTS

1 OVERVIEW

The goal of this paper is to provide technical guidance and information to college and university CIOs and CTOs, as they consider and adopt techniques to reduce illegal file sharing (Appendix C) on their campuses in the context of the Higher Education Opportunities Act (Appendix B).

This paper updates and extends information gathered in 2008 by the Joint Committee of Higher Education and Entertainment Communities[1], which at that time was interested in learning more about vendor solutions to reduce the unauthorized distribution of copyrighted materials.

The authors hope this up-to-date distillation will make it easier to identify and adopt technical solutions for a variety of campus networks – the paper considers a range of technical possibilities to cover as many network topologies as possible.

Briefly, general technical approaches to reducing piracy along with examples are described in Section 2 and detailed in Section 3. Comments on other situations campuses may face can be found in Section 4. A list of vendors and products referenced in these sections can be found in Appendix A. The goal is to identify vendors and we make no endorsements.

It's important to note that while CIOs/CTOs often think in terms of new equipment, the authors found that existing equipment may often be readily used to address illegal file sharing – in many cases, basic technologies are useful for both network management/security and reducing copyright infringements.

The authors note that technology is only one aspect of a program to reduce illegal file sharing. Other components necessary for an effective program include copyright awareness and education. Note that critical legal and policy issues not addressed by this document are explored in numerous other references and can be found by following links in Appendix E.

[1]Information about the Joint Committee can be found here:
http://www.educause.edu/EDUCAUSE+Major+Initiatives/JointCommitteeoftheHigherEduca/1204

2 GENERAL TECHNICAL APPROACHES

In this section, we identify five broad categories of technical approaches that may be used to combat copyright infringement:

Broadly categorized, Security Information and Event Management (SIEM) and Advanced Monitoring Solutions (AMS) recognize infringing activities and provide the technology and tools which can be used to implement graduated response. Both SIEM and AMS are generally passive technologies.

Web filters and inline monitoring and IDS/IPS solutions recognize infringing activities and can provide the technology and tools to implement a graduated response. These technologies can also actively block the infringing activities.

The following table highlights some considerations when deciding on a technology.

Campus Goals	Approaches to consider	Technologies
$0 budget	Use what is on campus, particularly IPS, to block peer-to-peer (P2P) file sharing. Potentially use local DNS and firewalls to do simple site blocking for cyberlockers and streaming sites. If there is no technology available, consider SIEM or AMS to identify issues and address them via help-desk. Strict consequences generally mean fewer incidences.	Existing campus technologies, particularly IPS and DNS. Use SIEM (Snort[2] is free) and AMS BAYU[3] is good if you have the hardware to support it.
Can deploy equipment, but staff overworked	Consider solutions that 'block' illegal file sharing, in particular P2P and site blocking.	AMS, particularly systems that respond to violations. Inline blocking and IPS can virtually eliminate unwanted activities. Advanced Firewalls may also meet your needs.
Staff, but no equipment	Emphasize graduated response. Detect policy violations and then act upon them.	SIEM, AMS to detect violations. BAYU to inform users. Automatically process notices with Automated Content Notice System (ACNS).
Practical, reliable solution	The best approach is a combination of technologies to detect violations and a graduated response program emphasizing education and consequences for actions against your college or university's network-user conduct policies.	Inline systems and AMS intelligently detect unwanted activities which can be handed off to BAYU or graduated response. Some behavior might be excessive and merit 'blocking' outright, which can be done with inline systems, IPS, DNS, or advanced firewalls.
Be a thought leader	For you, P2P is the easy part with many solutions. Challenge is effectively controlling download and streaming, but balancing these efforts with partial site traffic freedom. Consider site blocking when/if incidents arise that either are against your college or university's network-user conduct policies or which otherwise adversely affect the operability of your campus network. Also challenging are servers on campus networks. Rotate lightweight solutions through campus to look for violations. Potentially put the responsibility on the student by having them opt-in to various access situations.	Opportunity is intelligent integration of different technologies.

[2] Snort (www.snort.org) is a free intrusion detection/protection system.
[3] Be Aware You're Uploading (BAYU), http://bayu.umich.edu/

It is important that goals be realistic and to recognize that the goal for technical measures is to *reduce* illegal file sharing and not to eliminate. It's also important not to be distracted by information concerning the robustness of any solution surrounding illegal file sharing. There are countermeasures for almost every technology described in this paper. However, in practice the above techniques have been proven effective at colleges and universities across the country. It will require work and diligence, but in the end you can create an effective and manageable system. It should also be noted that many corporations use very similar techniques to limit the access of their employees to engage in similar or even more expansive activities (e.g. access to social media sites).

We recommend that any solution selected have mechanisms that allow community members to opt-in to obtain access to restricted technologies and sites for non-infringing uses. The opt-in can range from an automated mechanism (for example, a click-through "day pass" for P2P) to a more generalized approach (for example, terms of use permitting students to use P2P if they're willing to accept more severe sanctions if they receive a DMCA notice).

2.1 Security Information and Event Management (SIEM) and Network Behavior Analysis (NBA)

SIEM is a low cost, entry-level approach to reducing copyright infringements on campus. Created over a decade ago, SIEM technology compiles "transactions" or "events" generated by systems, applications, databases, and network devices such as routers, switches, and hubs.

Summaries of network events are collected and analyzed to determine what's happening on the network. This enables network administrators to create alarms that signal certain network conditions (such as specific events or when particular thresholds are reached) that you and your professional staff will want to address. For example, a systems administrator might set a threshold on the maximum traffic per day to individual computers on the residential network; if this were exceeded, it would be considered an event.

While traditional log management tools exist, SIEM is a superset of functionality, which includes not just logs, but event interpretation, and analytics to determine proper courses of action based on those events.

Pros	Cons
• Offers a low cost entry point for various types of reporting and compliance. • The device that accumulates these logs does not need to be "inline" and thus does not add overhead to the LAN traffic or affect reliability. • Offers other value to the network, including managing server events (i.e. the server event logs). • Patterns can be established over long periods of time. Customizable analytics and reporting. • Works well with non-authenticated users. • Ability to set threshold identities to filter out false alerts. • Seamlessly works with cloud-based services and mobile devices, assuming availability of logging.	• Devices must be configured to produce and write logs. This is relatively basic, but assumes that the device does indeed produce an industry standard log. In addition, this adds 1%-5% overhead on the device itself. • Can only determine a subset of security breaches. • Does not take remediation steps, only reports alerts based on set thresholds or tagged events unless paired with an IDS/IPS. • In order to leverage the true power of an SIEM, routers and switches should support NetFlow™ or sFlow® inherent in Cisco®, Brocade®, Extreme®, HP® ProCurve, Enterasys or Juniper® network environments.

• Leverages a university's investment in existing routers/switches by turning them into "virtual monitors," while eliminating the need to put a costly probe or appliance on each segment of the campus network. • Analysis can be implemented in less than an hour—no network downtime needed to install or run. In the case of NBA (Network Behavior Analysis) context of the traffic or transgression is also available.	

2.2 Advanced Monitoring Solutions

These types of advanced monitors and inspectors are able to build detailed pictures of your LAN/WAN traffic, its usage and its sources and destinations without being an "inline" device.

Although monitoring can be done on a more aggressive level (see web filters) and can trigger immediate actions based in real time, AMS generally involves passive inspection and monitoring.

Pros	Cons
• Does not require a large investment in time or resources. • Can be implemented in amost any environment. • In no case can the system hamper or impede traffic flow as a web filter can. Devices do not need to be touched or modified for this solution to work. • In some solutions, an appliance in this space can be upgraded to be an inline (web filtering) solution at a later date. • These devices monitor each computer's real-time bandwidth, with alarms. Also addresses other technologies like Instant Messaging. Can identify applications being used. • Works well with non-authenticated users. • Harder to "fool" than an SIEM, and can detect many encrypted and obfuscated communication types.	• Although alarms and thresholds for alerts can be programmed, actions on those alerts are manual unless the system is integrated with a response system. AMS devices do not by themselves stop unwanted traffic or applications, but rather report on it. An institution must either have an automated system or be adequately staffed to respond to events. • Requires that the network admin utilize the reporting system. • Most AMS solutions expect a "mirror port" on the core switch for monitoring data availability

2.3 Inline monitoring, protocol filtering, web filtering and traffic shaping

These types of advanced monitors and inspectors are able to build elaborate and complex picture of your LAN just like an AMS, but offer a more complete set of functions because they sit in-line with a firewall or IDS device. There are a large number of solutions that fall into this category and many have been implemented on hundreds of campuses.

This is a sophisticated level of monitoring, capable of immediate real-time actions to stop undesired traffic. This can include shutting down a port, blocking an IP address or NIC, or rerouting certain traffic to an "island" or containment-and-remediation portal. This is a complete solution, but

stops short of being an Intrusion Detection/Protection System (IDS). Note that some of these solutions incorporate NBA.

These solutions offer the ability to block unwanted traffic, providing a high level of control. However, this is a more proactive and intrusive approach to shaping traffic with associated risks. As such, these solutions have 'enterprise-level' availability and quality. Most have extremely high availability (at least 5-nines) and pass-through fail-safe modes. They also, typically, have enterprise-level pricing.

Pros	Cons

• Most complete analysis which also can offer real-time automated remediation actions.
• Can also stop or shape most other traffic types including Instant Messaging and streaming.
• Devices can be used in AMS mode and moved to inline at a later date.
• Vendors in this space are going to offer complete solutions. Some solutions are specifically targeted at colleges and universities.
• Most implementations are also able to "message" endpoints and alert them that you are aware of the transgressions, encouraging self-remediation.
• Web-filters with blacklists help stop a large amount of virus, bot-net, and virus outbreaks.
	• The following inherent risks of in-line devices are low, but must be considered when evaluating these solutions
	  ○ Can cause unexpected issues with technologies as the packets are being "opened" in-route (rare, but possible)
	  ○ Overhead can sometimes cause traffic delays. Typically, this is not a problem, especially on residential networks, but on high-performance research networks, the behavior should be well understood before proceeding with this approach.
	  ○ When an inline device fails, it can interrupt traffic flowing through it. However, inline devices are designed for high availability and the track record on these devices is excellent.
	• Requires solution engineering and engagement resources from the vendor to implement.
	• Implementation, which enables remediation actions such as redirecting a port, can be hardware dependent. Solutions often support NAC (Network Access Controls,) which can be used to toggle user access at a granular level based on network or AAA information.
	• Blacklists must be selected and approved by you, and maintained; typically by vendors

2.4 IDS/IPS (traffic blocking)

An Intrusion Detection System[4] (or IDS) monitors network and/or system activities for malicious activities or policy violations. Intrusion Prevention Systems[5] (or IPS) add the ability to proactively determine a response to a detected intrusion.

In other words, an IDS is a passive system that reports security breaches, while an IPS reacts and blocks harmful traffic in real time. Unlike firewalls, an IPS both looks at inbound traffic and looks for any sort of intrusion (even within the network) based on heuristics and signature patterns. As noted, it typically responds by blocking access to the offending endpoint.

[4] http://en.wikipedia.org/wiki/Intrusion_detection_system
[5] http://en.wikipedia.org/wiki/Intrusion_prevention_system

Depending on where the IDS/IPS is located, it might be variously called a Network Intrusion Detection System (NIDS, protects an entire network), a Host-based Intrusion Detection System (HIDS, protects a single host), or a Perimeter Intrusion Detection System (PIDS, edge of the network) [6].

IPSs can be very good at identifying types of traffic and can therefore be configured to respond to that traffic as an 'intrusion'. This makes some IPSs excellent at blocking P2P. Furthermore, this blocking can be configured to allow P2P for some while making it unavailable for others. Many have found IPS useful to block P2P on unmanaged wireless networks.

Pros	Cons
Many campuses already have an IPS in their network for protection against malicious traffic. We investigated and confirmed specific examples of TippingPoint and Red Lambda where campuses successfully addressed file sharing on campus. We suspect other vendors have been similarly effective. • Not just a traffic-based solution, an IDS also is a large component of network security and protection. • If assets already exist on P2P blocking with 'opt-in/out' can be implemented without a large additional investment. • Able to integrate with SIEM solutions for a 2-pronged approach. • Able to correlate and make decisions based on data gathered from the entire network, not just from single points.	• Inline solution (see Cons of inline solutions in section above.) • Next generation firewalls are adopting functions traditionally considered IDS/IPS. It's worth considering next generation firewalls when considering IDS/IPS. • Will require regular ongoing vendor support due to complexity.

2.5 Web Site blocking

Web Site Blocking (aka Site Blocking) is the act of preventing an endpoint (or a user on an endpoint) computer from communicating with a specific set of destination endpoints. Depending on how the user accesses a blocked site (e.g. web browser or from an app), the user would be prevented from reaching the site and instead either be presented with an error condition or redirected to a substitute page (e.g., warning message)[7].

If the blocking is performed via DNS, then redirection should be avoided to avoid conflicts with DNS Security Extensions (DNSSEC). If blocking is implemented at the IP address level, then redirection is quite doable. In fact it is quite commonly done in applications such as free airport WiFi.

[6] http://en.wikipedia.org/wiki/Intrusion_detection_system#Types_of_intrusion_detection_systems

[7] Redirection of a web or app request if done at the DNS level is currently a violation of DNSSEC and should be understood as not a preferred method of dealing with site blocking efforts.

Pros	Cons
• In some variants, requires no specialized appliance hardware • Quickly discourages the casual user • Works just as well with unknown users. • Non-intrusive solution	• Solutions can be in conflict with other solutions or components and standards of the internet. • The simplest methods can be circumvented • Blocking lists management are a challenge themselves

2.6 Other Alternatives: Next Generation Firewalls

Next Generation Firewalls combine traditional firewall capabilities with other functions, such as those described above. These devices incorporate numerous technologies such as intrusion prevention methods, network behavior analysis and firewalls. Others support additional functionality and interoperability with IPS and SIEM devices in real time.

Last year, Gartner recommended that enterprises migrate from stand-alone IPS to next-generation firewalls for performing IPS functions[8]. It's unclear whether this is the future of network security, but these advanced appliances can secure both inbound and outbound communications.

Pros	Cons
• Combines the best of both security worlds, a firewall with built in IPS. • Can be deployed inline or as a proxy server. • Combines very well with authentication scheme solutions, which are on the horizon.	• Emerging technology—many products are still maturing. • Costs are still higher than other solutions. • Will require regular maintenance from staff or vendor. • As with any inline device, failure of device takes down entire network. However, as with other inline solutions, these are designed for high availability. • Still an emerging market.

2.7 An Integrated Approach

The solutions described above illustrate implementations of specific technologies in isolation. In practice, many have found it beneficial to deploy heterogeneous solutions.

Combining approaches can create a computing environment that effectively detects issues, identifies participants and provides suitable teachable moments and consequences. Approaches that provide multiple options allow an informed community to participate in deciding which technologies and internet access are most suitable for them.

[8] http://blogs.gartner.com/greg_young/2009/10/15/defining-the-next-generation-firewall-research-note-the-liner-notes/

3 EXPANDED TECHNICAL INFORMATION

In this section, we provide additional technical detail for those involved in planning an approach.

3.1 Security Information and Event Management (SIEM) and Network Behavior Analysis (NBA)

SIEM technology compiles "transactions" or "events" generated by systems, applications, databases, and network devices such as routers, switches, and hubs.

Summaries of network "events" are called "event logs", and these can be analyzed to determine what's happening on the network. This enables network administrators to create alarms signaling certain network conditions (such as specific events or when particular thresholds are reached). For example, a systems administrator might set a threshold on the maximum traffic per day to individual computers on the residential network; if this were exceeded, it would be considered an event.

Network behavior analysis (NBA) compliments SIEM by looking for unexpected changes in network behavior.[9] For example, NBA can detect servers operated in violation of the campus Terms of Use because server traffic is anomalous. Looking ahead, next-generation SIEM solutions are being augmented by NBA functionality.

SIEM includes not only logs, but event interpretation, and analytics to determine proper courses of action based on those events.

3.1.1 Target Environment

SIEM is well-suited for smaller network footprints and topographies that have some "managed" devices (for example, devices that support typical network diagnostic software such as Netflow, sFlow, event logs, et al.). In practice, most network devices support logging – the lowest performance level needed – and that includes wireless routers.

In terms of capabilities, SIEM enables analysis of traffic patterns and flows and provides less information than advanced monitoring systems (AMS), which use deep-packet inspection to identify applications and, in some cases, copyrighted content. Still, SIEM should be approximately 80% as effective as AMS.

3.1.2 Example: SIEM (Using Lancope)

SIEM is a fairly broad category and its use and capabilities are best illustrated through a specific vendor solution: Lancope StealthWatch.

StealthWatch is a representative next-generation SIEM solution that includes NBA. It targets detection and identification of defined types of network activity and is used more for network analysis than immediate network management. This enables colleges and universities, for example, to document network activity that may have triggered a notice.

[9] Network behavior analysis also works well with IDS/IPS, firewalls, and other approaches to network security.

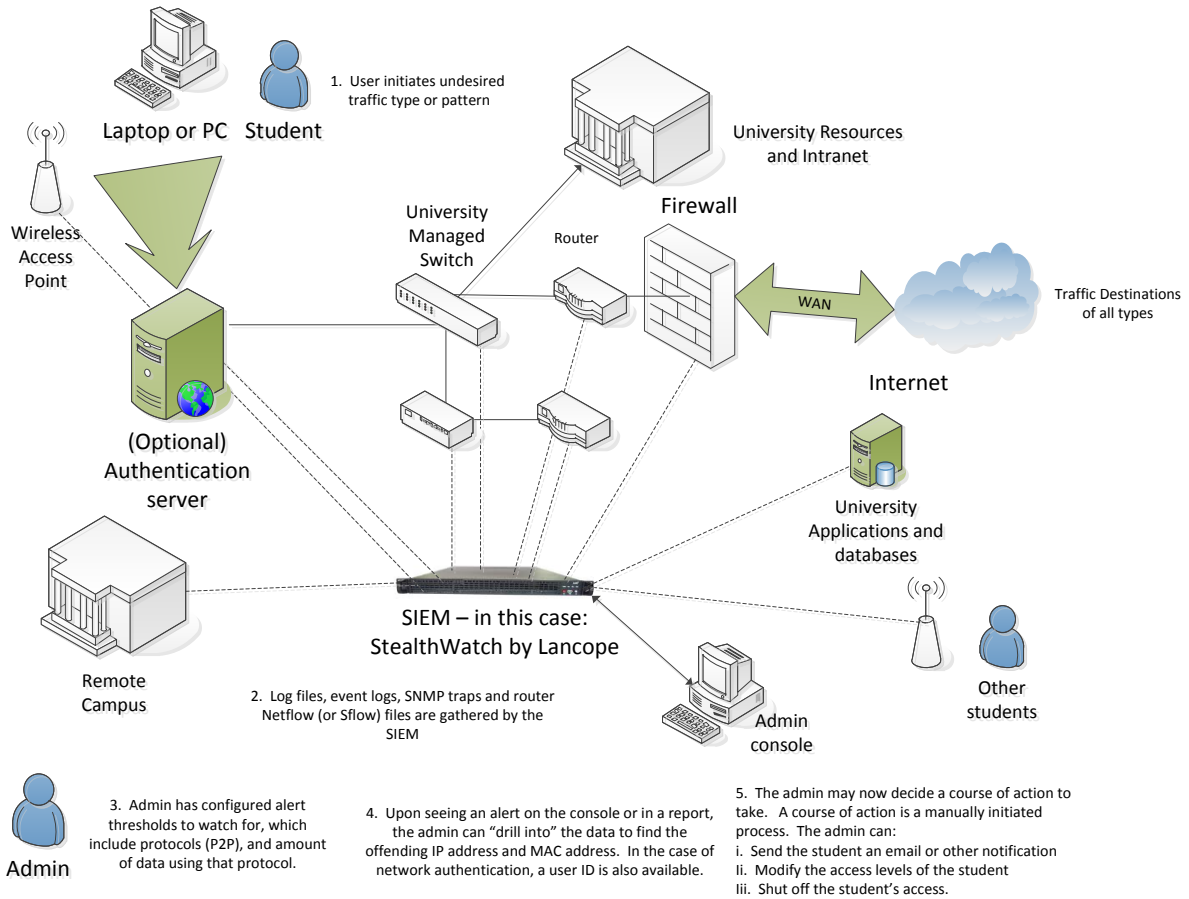
This scenario would be used to detect behavior on campus that could be in violation of a campuses' acceptable use policies, such as use of protocols that are frequently used for piracy, (for example, peer-to-peer [P2P] file sharing), or for access to illicit sites. The response is up to those administering the system.

Lancope's "out of the box" StealthWatch NetFlow collector collects flow data from routers but does not receive or examine full packets or their content (thus, it examines only Layers 3 and 4, which for IP includes the end point addresses and ports, and does not do deep- packet inspection). Lancope does offer optional tools (FlowSensor AE/VE) that permit full packet capture – these packets may then be examined with DPI should an administrator desire more detailed information about traffic and traffic types.

Universities can purchase these optional tools to protect the campus network—for example, to provide email/SPAM source alarms. They may also be used to address copyright infringements on campus.

For example, the Layer 7 application identification capability may be used to look for traffic indicative of file-sharing activity (including peer-to-peer file sharing applications such as bittorrent). False positives are mitigated by properly "tuning" the monitoring algorithm to create the proper "threshold" for inspection and reporting.

The diagram below, illustrates how SIEM may be used on a university IT network.



Technical and implementation details are as follows:

- Usually at least 2U of rack space is needed for StealthWatch and IP addresses for StealthWatch appliances need to be reserved, as does DNS, NTP server, and the like.
- One must put in the necessary change requests to turn on NetFlow/sFlow/IPFIX and export it to the IP address of the StealthWatch Flow collector. This would also include setting up SPAN ports (only if using optional DPI FlowSensor). Additional considerations include where in the network to collect flow information, for example, core switch vs. the edge and distribution layers. If there are multiple campus locations, one may want an individual flow collector at each location vs. sending flow data across the WAN.
- Internal and public IP address schema need to be put into a spreadsheet for automatic importation into the StealthWatch Management Console (or keyed manually) for the StealthWatch Zone structure.
- Plan for a two-hour installation maintenance window (though it should take less than an hour).
- Plan to spend two hours a week for the first four weeks to ensure that the StealthWatch system is tuned and configured for the network. Since StealthWatch is a learning and base-lining solution, it does take a couple of weeks to learn your network (though it can begin to identify P2P activity from the first hour).
- Formal training is a one-day class best attended after the first four weeks described above.
- At 60 days (a month after the formal training class) it is best to perform a StealthWatch system check and Best Practices session; this can usually be conducted online free of charge with Lancope.

3.1.3 Other considerations

As a low-cost, entry-level solution, this approach is well suited for smaller budgets. The appliance is non-intrusive and, while lacking an automated response mechanism, does enable the university to monitor network use while respecting student privacy and minimizing costs.

This approach also works with existing firewall technology and does not require an embedded IDS/IPS to be effective. Additional benefits include the capability to detect, then quickly and effectively track down and eradicate virus or worm type outbreaks.

Because tuning of thresholds is involved, administrators should expect to spend some time tuning the appliance via the management console.

SIEM often requires additional information about network configuration. Anomaly detection typically occurs at the level of switch port, MAC address and/or IP address. For action to be taken, knowledge of equipment allocation is necessary to map an alert to a device or user.

A key benefit of the basic SIEM solution is that it provides visibility into network activity while avoiding the issue of privacy – which some feel is threatened when DPI is used. SIEM identifies only IP addresses (and hence users) and relies upon historical network data (assuming it's retained) to support forensic investigations of alleged behavior.

3.1.4 Representative Vendors

ArcSight, Lancope, LogLogic, Q1 Labs, RSA, SenSage, Skybox, Snort (as monitor), Sandvine.

3.2 Advanced Monitoring Solutions

These types of advanced monitors and inspectors are able to build detailed pictures of your LAN/WAN traffic, its usage and its sources and destinations without being an "inline" device.

Although monitoring can be done on a more aggressive level (see web filters) and can trigger immediate actions based in real time, AMS generally involves passive inspection and monitoring.

3.2.1 Target

An AMS is a mid-level solution that provides a better feel for network utilization and concerns than SIEM. An organization with any size footprint that is interested in monitoring and reporting specific types of traffic and usage (such as P2P traffic and applications) can utilize this with minimal impact on existing infrastructure. Reporting is typically robust and reports are used to make decisions on what issues should be followed up on and what those actions will be; thus there are staff requirements associated with the solutions. This is a good fit for a campus looking to work with an Automated Copyright Notice System. In some cases, vendors already incorporate this functionality.

AMS is slightly more expensive than SIEM and may be slightly more intrusive in its oversight.

3.2.2 Solution Type and Application

AMS is similar to SIEM in application, but since such systems are more complete solutions they can be used in environments where more specific monitoring is required. AMS offers more of a fine brush relative to SIEM's broad brush.

BayTSP (now Irdeto), a slightly different type of AMS, offers the capability to monitor activity, particularly P2P, external to your network in a manner similar to that used by rights holders to generate DMCA notices. They can monitor your network before and after you make changes to determine whether those changes are effective.

AMS systems are often tied to actions, making them suitable for applications such as graduated response. In other words, these systems monitor traffic, but await administrator-designated thresholds before redirecting the user to an isolated Remediation Server where the user can learn what policy was violated and what corrective action may be necessary. The Remediation Server (aka Graduate Response website, aka sanctioned user website) has instructions as to what steps must be taken for access to be restored, as well as information and alternatives to downloading. The Remediation Server is a campus server, behind the firewall and would not be reachable by outsiders. For this reason, it is the best of the AMS type solutions.

If an inline solution is in the long-term plans, many AMS systems can be run in passive mode and then converted to inline use in the future. If considering inline for the future, consider AMS now.

3.2.3 Impacts

AMS systems are by and large passive monitoring systems and have little impact on network traffic. There is normally a minimal amount of maintenance and administration. In this case, the administrator would define the thresholds for alarm (or accept recommended default values). When these thresholds are exceeded, an alert will notify the administrators and, in the case of a solution capable of a graduated response, also isolate the traffic of the transgressor. Remediation can be self-service or manual.

Colleges and universities implementing this type of solution are looking to notify users of transgressions in the hopes that notification of policy violation(s) is enough to stop the unwanted activity. If the transgressions continue, access can be blocked, reduced, or in the case of Audible Magic, relegated to a safe harbor (aka remediation site).

As one transitions from SIEM to AMS the monitoring becomes more detailed. In particular, it examines in more detail the contents of packets. Some campuses may have policies against such monitoring and therefore might be obligated to opt for SIEM.

3.2.4 Representative Vendors

ipoque, Riverbed, Audible Magic, Irdeto.

3.2.5 Example: AMS Out-Of-Band (Using Audible Magic)

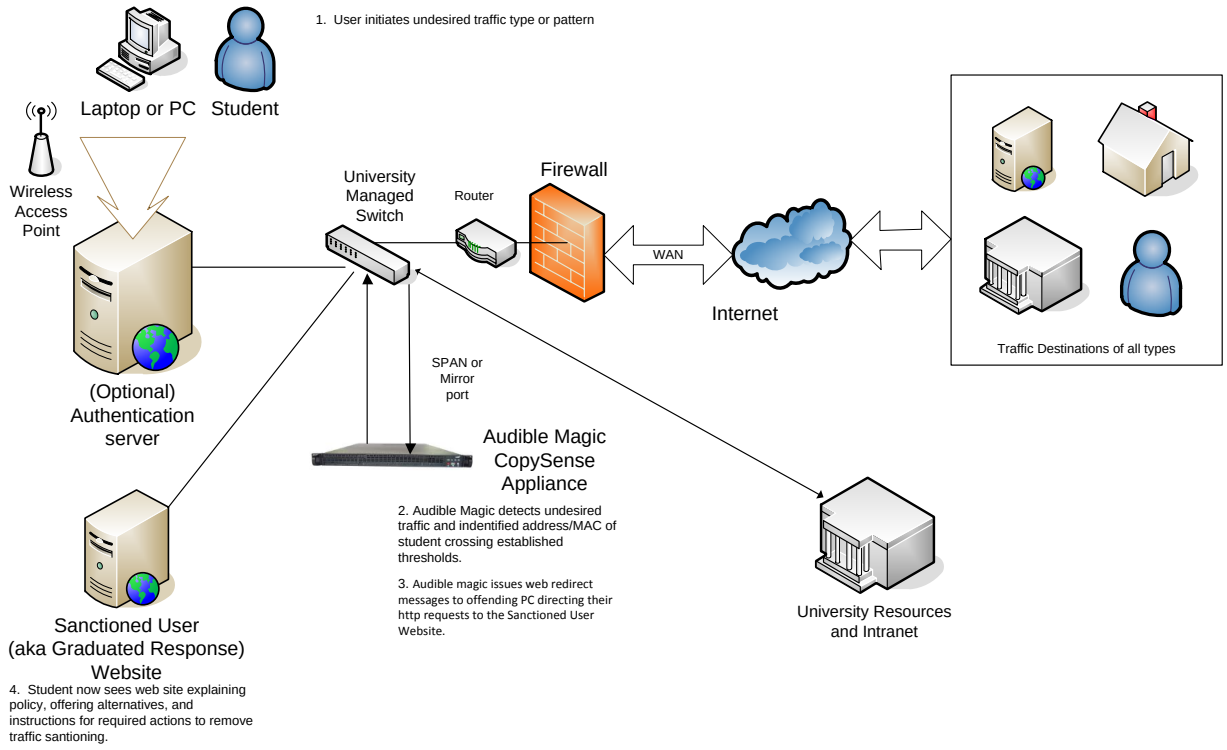
To illustrate Advanced Monitoring Solutions we offer the following as an example using Audible Magic. This example shows a variety of deployment options ranging from just monitoring to a fully responsive system.

The Audible Magic CopySense appliance is capable of identifying packets containing copyrighted material, and of intelligently deciding whether this use violates a network policy (for example, using P2P to transfer media).

This level of inspection is an excellent solution for campuses that want to respond to specific violations rather than more blunt solutions such as BAYU or P2P blocking that addresses all traffic of a specific type. As with most systems, there may be incorrect indications of misuse, so an opt-out policy should be implemented—it is supported by CopySense.

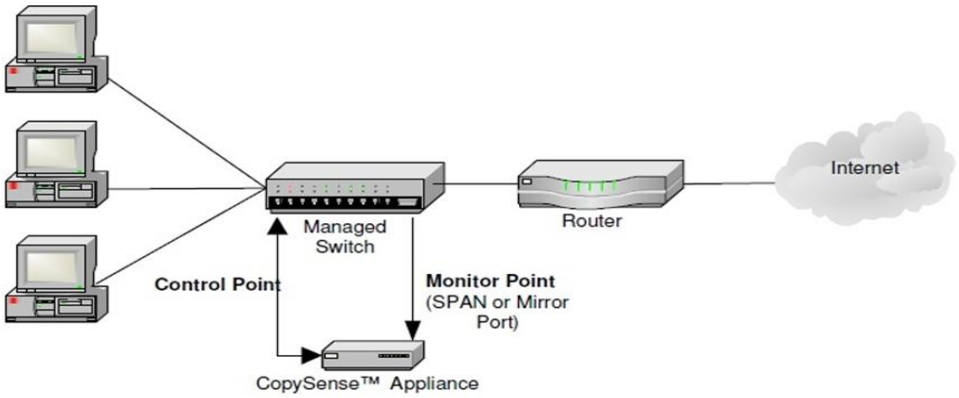
The following illustrates that the CopySense appliance is connected at a point where it can monitor traffic between the campus and the Internet, typically a switch or router near a firewall. The appliance monitors packets, not just Netflow.

When the CopySense appliance detects a Terms of Use violation as configured, it can report the information and/or isolate the user by a web redirect. There are numerous options here, including integration with an event management system, browser redirects forced by CopySense, browser redirects through a system such as FrontPorch, or integration with BAYU.

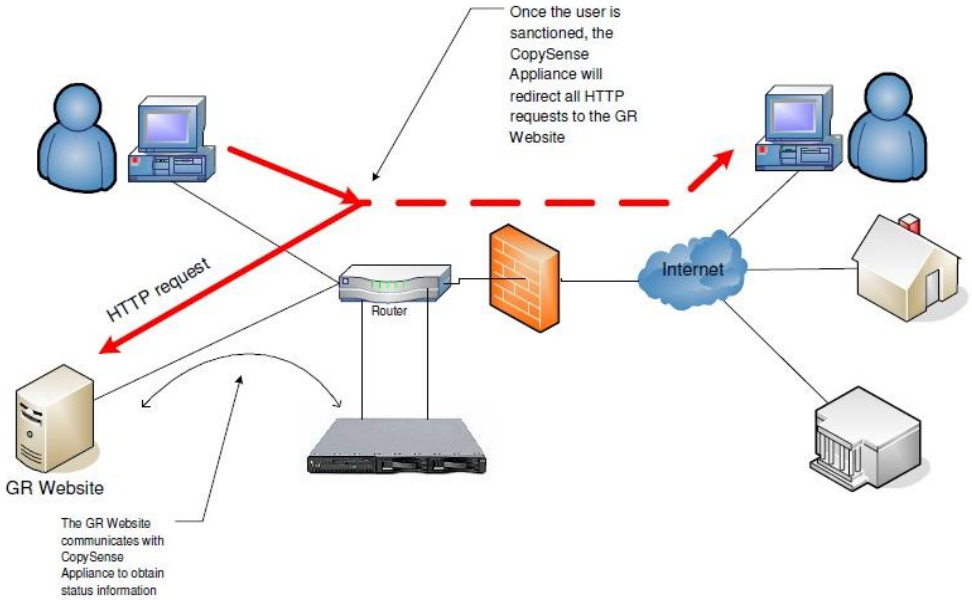


The following diagram provides more detail about the CopySense connection to the network.

It connects at a point on the network that carries network traffic you want to monitor, typically at the edge of the network, although it could also be internal if excessive inappropriate traffic is suspected. The CopySense appliance NIC is connected to the monitor point and is passive, that is, it only receives traffic. As it is not inline, it cannot interfere with network traffic. Managed switches typically have a 'monitor port', 'mirror port', or in Cisco parlance a 'SPAN' (Switched Port Analyzer) port where the CopySense appliance connects. The switch is configured to send packets to this port. In the case of a router or unmanaged switch, SNMP messaging can be used.



Audible Magic offers an integrated graduated response solution, as illustrated in the following diagram. It works as follows: The graduated response website is a local website that you deploy and that is under your full control. Once a user is sanctioned, the CopySense Appliance will continue to redirect that user's browser to the graduated response website until you manually or programmatically instruct the CopySense Appliance to unblock the user. The graduated response website is where you can educate the user about proper network usage and copyright laws, and ask for their compliance. Once you are satisfied with their response you can programmatically instruct CopySense Appliance to stop blocking the user. To aid in quickly developing a graduated response website, Audible Magic provides a sample web site (there are ASP.NET and PHP versions).



Following are some considerations related to this example:

Audible Magic states that although each installation is a bit different, setup can be done on the phone in about an hour.

Nevertheless, you should expect to work with the vendor for a couple of weeks for configuration.

- You will need to put in the necessary change requests to configure and utilize your core switch span port.
- In order for the redirection to work, there needs to be a landing page (aka website) for that redirect. There will need to be a web site provisioned and configured for this purpose. Expect to spend a couple of weeks on this.
- In the off chance you don't have a monitor or SPAN port on the core switch, the alternate methods of implementation are not as effective. You would be served better to upgrade the core switch.

3.3 Inline monitoring, protocol filtering, web filtering and traffic shaping

These types of advanced monitors and inspectors are able to build elaborate and complex picture of your LAN just like an AMS, but offer a more complete set of functions because they sit in-line with a firewall or IDS device. There are a large number of solutions that fall into this category and many have been implemented on hundreds of campuses.

This is a sophisticated level of monitoring, capable of immediate real-time actions to stop undesired traffic. This can include shutting down a port, blocking an IP address or NIC, or rerouting certain traffic to an "island" or containment-and-remediation portal. This is a complete solution, but stops short of being an Intrusion Detection/Protection System (IDS). Note that some of these solutions incorporate Network Behavior Analysis (NBA).

These solutions offer the ability to block unwanted traffic, providing a high level of control. However, this is a more proactive and intrusive approach to shaping traffic with associated risks. Consequently, these solutions have 'enterprise-level' availability and quality. Most have extremely high availability (at least 5-nines) and pass-through fail-safe modes. They also, typically, have enterprise-level pricing.

3.3.1 Target

As these solutions tend to be expensive, they are more suited to larger footprint campuses desiring real-time automated stoppage and ongoing prevention of unwanted traffic. In addition, this type of solution attempts to eliminate unwanted activity and thus is a good fit for a university with a zero-tolerance policy.

Colleges and universities that desire to insure that only sanctioned traffic is on their networks may wish to implement this solution. It will be the most exhaustive and far-reaching approach to the issue of unwanted traffic, and is accompanied by a stance that traffic on the university's network is university business and can legitimately be monitored and controlled.

3.3.2 Solution Type

This is a prevention solution type as the intention is to block unwanted behavior at the source in real time. In theory, once it is configured and deployed, risk of transgressions is minimal. Some even support customization of the detection filters, so that you can be very aggressive on some traffic and not so aggressive on others. Institutions that block or tightly control illegal traffic tend to get few, if any, DMCA notices.

Traffic shaping prioritizes different types of network traffic according to institutional policies, for example to ensure email remains unimpeded regardless of network load. In the illegal file sharing context, it can be used to lower the priority of protocols typically used for file sharing. Often this works in tandem with an IPS. Limiting bandwidth on certain protocols discourages illegal file shares by delaying gratification, and reduces the amount of material illegally shared from the campus network. As with most techniques, traffic shaping can be managed to allow certain IPs to get full bandwidth, regardless of other policies. More and more, traffic shaping is shifting to next generation firewalls (See 2.5).

Web-filters maintain lists of "blacklisted" sites and block access to those sites. This feature is important with the emergence of malicious site lists found both for malware and for various illegal activities.

3.3.3 Impacts

Overall, many institutions have found this approach to be a valuable part of an overall network management program. Traffic shapers can ensure that priority traffic (such as email) is passed while lower priority traffic (streaming video) is appropriately prioritized in the event of congestion or when a class of traffic exceeds its allocation. This is particularly important with P2P protocols, which can bypass Internet traffic flow protocols and receive 'unfair' allocation of bandwidth.[10]

The negative impacts are more difficult to fully assess and describe. It should be noted that problems tend to be minimal and have not been a significant barrier to massive deployment of these solutions. Because of how web-filtering works, it can sometime block acceptable traffic. There are myriad settings for blocking traffic types, destination sites and URLs. Determinations can sometimes be erroneous, resulting in some unwanted results. For example, an error in a blacklist might cause a legitimate site to be blocked.

This is a higher cost, higher maintenance type solution. However, PacketShaper, in particular, has been effectively utilized at multiple colleges and universities and is a popular choice.

In cases where the solution includes QoS functionality, administrators can fine tune traffic flow controls and bandwidth allocations on a per application basis (such as VOIP). What this means is that instead of blocking certain traffic, you could instead reduce and discourage it by lowering its available bandwidth. Note that this approach does not necessarily reduce the number of notices received unless it dissuades a student from downloading[11].

Identification of user often occurs via queries to the authorization database (such as a RADIUS server) so there is integration required.

This type of monitoring almost always involves DPI (Deep Packet Inspection), although none of the solutions in this section look at the actual content, only protocol data such as headers and behavioral information such as timing and failed connections. This means that rather than just looking at TCP and IP headers, the application-level data of the packet is "peeked" at, and data is compared to signature type to help determine the type of content. Administrators should understand whether a particular solution is consistent with campus policy and consideration should be given to appropriate disclosures. Retention policies should also be considered as part of product selection and configuration.

3.3.4 Representative Vendors

Cloudshield, Sandvine, Allot Communications, Blue Coat (aka PacketShaper and Packeteer), Procera, Facetime, IM Firewall, Enterasys.

[10] P2P, particularly Bittorrent clients tend to open numerous connections inherently bypassing the TCP congestion avoidance algorithm that works per-connection rather than per-endpoint. Here is an article that tested uTorrent: http://www.digitalsociety.org/2009/11/analysis-of-bittorrent-utp-congestion-avoidance/

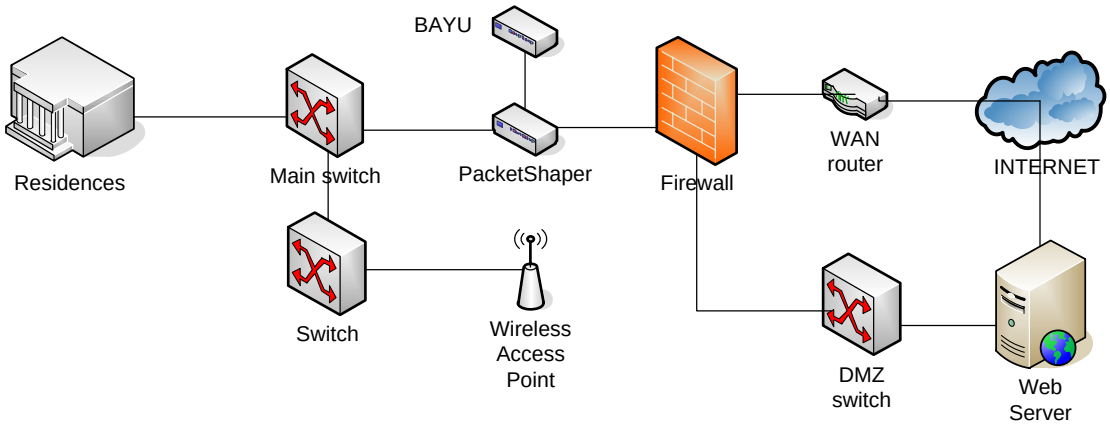
[11] A student illegally sharing *slowly* is still subject to a notice. However, slow sharing is unsatisfying and some students will be discouraged from illegally sharing, thereby reducing notices.

3.3.5 Example: Inline filtering and monitoring (Using Bluecoat PacketShaper)

Some campuses choose to limit the use of protocols used for file sharing, both because they use a disproportionate amount of network resource and because they are frequently used for illegal file sharing.

Bluecoat PacketShaper is featured in these examples, although it is only one of several products in this category.

In the following illustration, the PacketShaper is positioned inline, between the firewall and the backplane switch. As shown, the administrative and potentially the academic networks are not shaped, only the residential network and wireless network. This configuration also shows BAYU, which can integrate directly with PacketShapers (not shown is BAYU's integration with other campus systems).



Getting the most from a PacketShaper depends on choosing the right deployment strategy for your topology and needs. Typically, you expect to see either of the first 2 deployment methods in a campus environment but it does depend on factors such as the size of the campus, how many LANs, whether redundancy is required, control of DMZ bandwidth, and service providers to the campus. Other deployment configurations can be found on Blue Coat's site: https://bto.bluecoat.com/packetguide/8.3/products/entdeptopos.htm

Configuring inline filtering devices requires one to consider how bandwidth resources are to be used. For example, a PacketShaper allows protocols to be grouped and bandwidth to be assigned to each group. It also permits control based on IP addresses (either in groups or individually). Illinois State University's approach is instructive.[12]

ISU has created four traffic categories: Gold for mission critical (email, web, NTP, VPN), Silver (streaming, IM, gaming), Copper (iTunes, Flash), and Bronze (P2P, ping floods, virus traffic, DoS, and so forth).

Illinois State blocks traffic in the Bronze category though some campuses have chosen to limit P2P rather than block it.

[12] http://www.helpdesk.ilstu.edu/pdf/Network%20Bandwidth%20Management%20-%20October%202006.pdf

3.4 IDS/IPS (traffic blocking)

An Intrusion Detection System[13] (or IDS) monitors network and/or system activities for malicious activities or policy violations. Intrusion Prevention Systems[14] (or IPS) add the ability to proactively determine a response to a detected intrusion.

In other words, an IDS is a passive system that reports security breaches, while an IPS reacts and blocks harmful traffic in real time. Unlike firewalls, an IPS both looks at inbound traffic and looks for any sort of intrusion (even within the network) based on heuristics and signature patterns. As noted, it typically responds by blocking access to the offending endpoint.

Depending on where the IDS/IPS is located, it might be variously called a Network Intrusion Detection System (NIDS, protects an entire network), a Host-based Intrusion Detection System (HIDS, protects a single host), or a Perimeter Intrusion Detection System (PIDS, edge of the network) [15].

IPSs can be very good at identifying types of traffic and can therefore be configured to respond to that traffic as an 'intrusion'. This makes some IPSs excellent at blocking P2P. Furthermore, this blocking can be configured to allow P2P for some while making it unavailable for others.

3.4.1 Target

IDS/IPS is most suitable for organizations that need additional security and have funds for such initiatives, or those that already have IPS and wish to maximize use of existing resources.

3.4.2 Solution Type

This type of solution is focused on security first, traffic transgressions second. However, the more direct approach of blocking P2P and illicit sites (with suitable opt-out) can be very effective with little or no overhead.

3.4.3 Impacts

Since any solution in this space will be edge hardware, it can be expensive and require other equipment changes. Note: Red Lambda is a special case in that it does not require expensive hardware to implement. Instead it relies on internal distributed technology (what developers call 'grid') to utilize internal idle CPU cycles.

3.4.4 Vendors

Still Secure, Cisco (IronPort ASA), Endace, Enterasys, Red Lambda, HP (TippingPoint), Snort.

3.4.5 Example: IDS/IPS (Using TippingPoint)

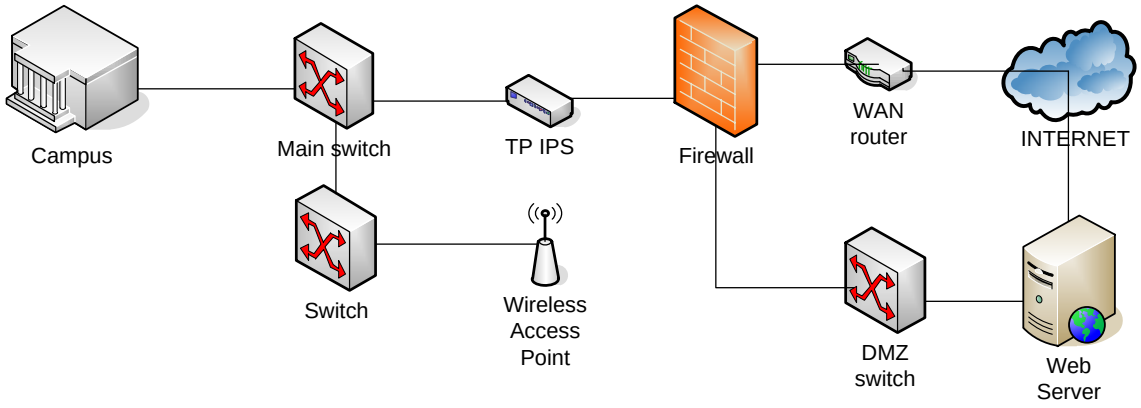
An IPS is a powerful tool for detecting and responding to all types of malicious behavior, including attacks. If a computer has been co-opted and has instigated behavior threatening

[13] http://en.wikipedia.org/wiki/Intrusion_detection_system
[14] http://en.wikipedia.org/wiki/Intrusion_prevention_system
[15] http://en.wikipedia.org/wiki/Intrusion_detection_system#Types_of_intrusion_detection_systems

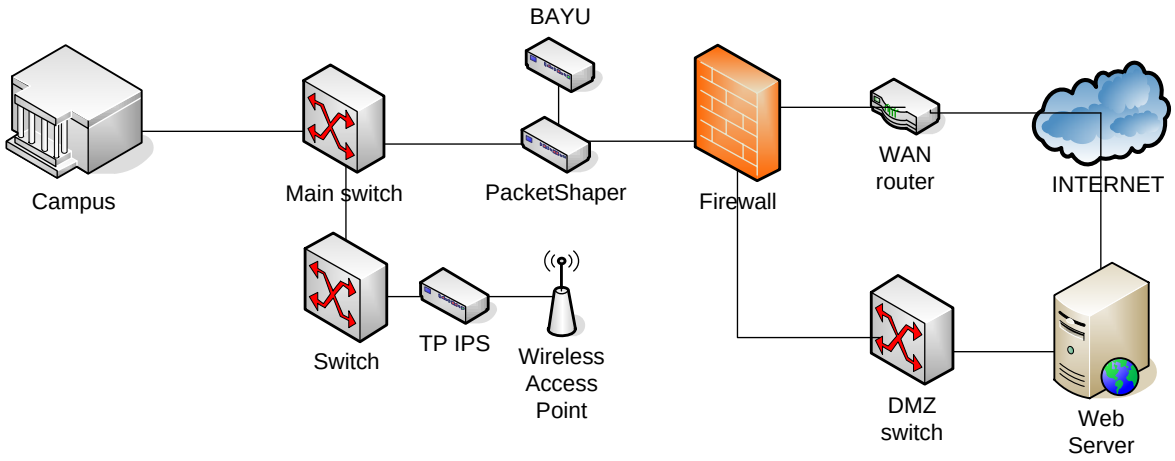
confidentiality, integrity or availability, an IDS can likely detect it, and an IPS can likely isolate it.[16] Because these functions are so important, many campuses already have an IDS or IPS.

The examples below feature HP TippingPoint, which is a popular choice on campuses, although other solutions are equally valid, including Snort, which is available in the public domain.

In the first example an IPS is used to block P2P. Although not in this exact configuration, Illinois State University has used TippingPoint to block P2P, virtually eliminating notices[17]. As shown here, a TippingPoint IPS appliance blocks all P2P on the residential and wireless networks. Administrative systems have direct access through the firewall.



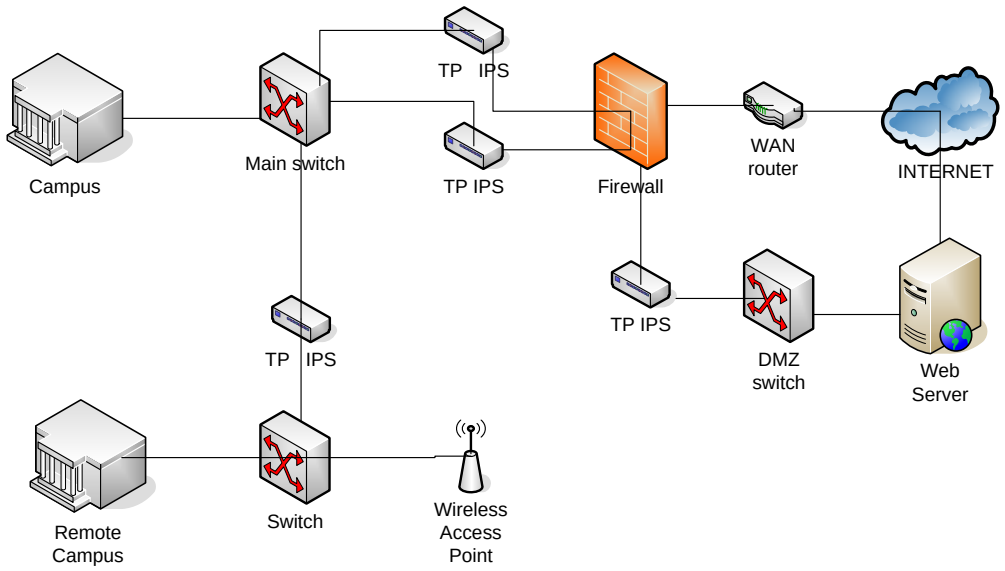
The next example uses TippingPoint to block P2P on wireless networks. Since the main network is not blocking P2P, a Blue Coat PacketShaper limits P2P while BAYU informs students if they are uploading and educates them on proper usage.



[16] Detection of all attacks is provably impossible, so no IPS solution should be considered perfect.

[17] Illinois State University has blocked P2P on residential networks since 2008 using a TippingPoint IPS, with an opt-in policy to facilitate legitimate uses of P2P. By virtually eliminating illegal P2P file sharing, this policy has virtually eliminated DMCA notices to the campus. http://www.helpdesk.ilstu.edu/kb/index.phtml?kbid=1432

The final example is a fully deployed IPS solution. This will identify other types of traffic, such as large servers on campus, typically used for illegally sharing files and often banned accordingly.



IPS units are generally inline so they can drop packets deemed harmful. IDSs can work in monitor mode since they are passive.

Two TippingPoint IPS Platforms can be provisioned using redundant links in a transparent High Availability mode. Because the IPS Platform acts as a "bump in the wire," lacks an IP address and does not participate in routing protocols, redundant TippingPoint platforms can be deployed in existing high availability network designs without changing the network configuration.

3.5 IP and DNS Site Blocking

There are multiple options evolving in this space. DNS Servers, firewalls, IDS/IPS, "Unified Security Gateways" and other systems have the capability to block access to sites. This capability often appears in corporations where management blocks access to sites such as social network sites, to avoid lost work time. Sites are also blocked for malware, phishing or criminal activity. There are both appliance and hosted versions of this solution. Middle and lower tier solutions in this space were originally developed for blocking pornography and have expanded and matured from there.

3.5.1 Blocking via IP

IP blocking prevents access to a particular set of IP addresses. It is simple conceptually, but difficult to manage because sites can easily move to new IP addresses[18]. IP blocking can work in either direction (ingress or egress). Inbound IP address blocking was originally constructed to protect web sites from brute force attacks from known hostile IP addresses designed to compromise data. Outbound IP blocking stops traffic to sites based on their specific IP address. Packets with the blocked IP address are discarded. IP blocking can be circumvented through the use of proxy servers

[18] When the move to IPv6 becomes more commonplace, IP blocking becomes an increasingly harder problem as the address space for IPv6 is enormous and it becomes more practical to make use of a large number of addresses.

that introduce an alternate IP address to the destination site. IP blocking can happen in the end system (e.g., a student's computer) or campus equipment.

IP blocking does not require deep packet inspection; that is, it only needs to look at the IP (layer 3) header. Many vendors categorize their solution in the web filter space.

IP blocking becomes more problematic with the switch to IPV6 as the virtually unlimited IP address space will make blocking specific IPs or ranges of IPs a much more complex problem. IP blocking would generally have to be combined with other forms of blocking to create a strong solution, such as constantly doing DNS lookups on any domains tied to the list of blocked IP addresses.

This solution is best focused on sites involved in streaming and non peer-to-peer traffic, although it is also useful for P2P servers such as bittorrent trackers and eDonkey servers.

Vendors in this space: Irdeto, Cisco, Juniper, Websense

3.5.2 DNS blocking

Domain Name System (DNS) is used to turn site names (e.g., www.veryharmfulsite.com) into IP addresses. DNS is served by a distributed infrastructure which manages domain and site names. DNS blocking prevents DNS requests from returning an IP address, making it difficult for a person to get to a site. For most people, if you entered www.veryharmfulsite.com and got back an error message, it's unlikely they would know how to get to the *veryharmful* site without technical help. Unlike IP blocking, DNS blocking does not have to worry about changing IP addresses. An organization would have to change its name to circumvent it, and a changed name would make them harder to find.

A more sophisticated user could circumvent DNS blocking by changing their DNS server entry to point to an "open" or "public" DNS server which is not participating in blocking domains. This is beyond most users' general ability and it has risk for those who take this route. It is also something that can easily be taught to another individual either by providing a simple download that updates your DNS or various plugins.

A straightforward approach to preventing the workaround for a larger user base is to prevent the use of other outside DNS servers. This is done by either blocking port 53 traffic or redirecting port 53 traffic to internal DNS servers. Blocking of outside DNS servers also will help with rogue DNS servers that either have been compromised or are fraudulent in operation from also being used for other malicious uses. Countermeasures to this are also possible but require a more sophisticated approach like the use of VPNs.

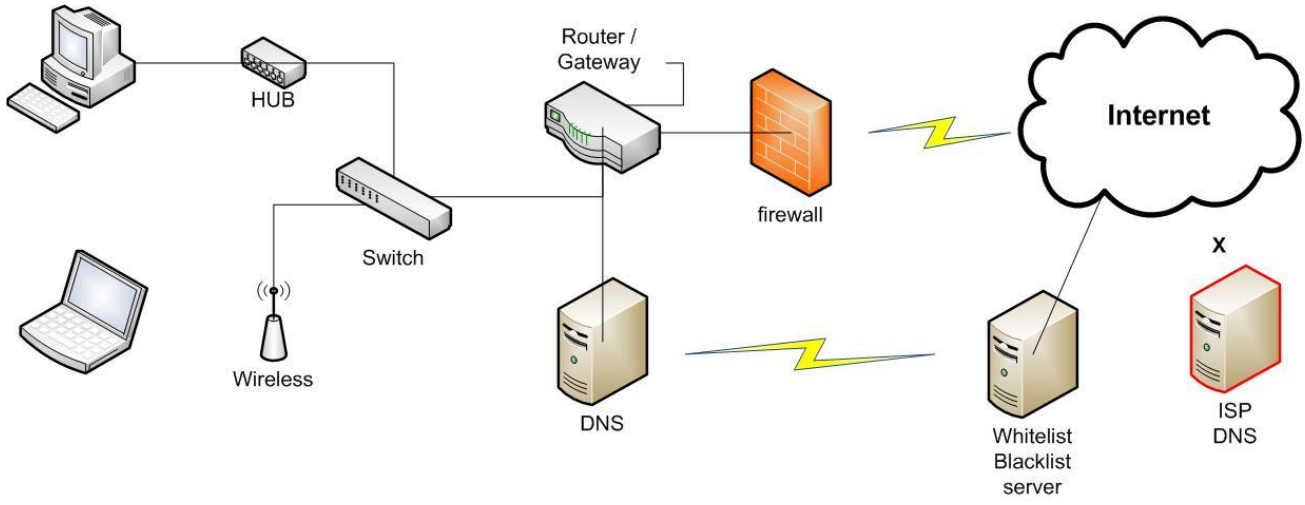
A variation of DNS Blocking is a DNS redirection. This substitutes the destination IP address with an alternative IP address that is constructed to explain why the request is not being fulfilled. As mentioned earlier, this can be an informative message about being blocked. However, there are complications with this last approach. DNS Security Extensions (aka DNSSEC) is a means of preventing DNS spoofing by requiring DNS records to be digitally signed. When implemented, malicious attacks on DNS requests would not be honored, thus preventing the hijack or spoofed destination. A side effect of DNSSEC implementations (still in early infancy) is that DNS redirection technologies used to combat misuse of internal resources, would have to be disabled or

removed, because a redirection (alternative IP address) is an inherent violation of DNSSEC. DNSSEC is described in more detail in Appendix D.

DNS Blocking is a simple tool generally straightforward to implement with current DNS solutions. Still, there are straightforward workarounds and the actual long term efficacy of such solutions is not fully understood. A more robust solution would add alternative DNS servers to the blocked list. This approach is more difficult circumvent.

Blocking solutions require current lists that indicate which sites are to be blocked. There are both public and private variants of these lists and one would need to align with a list provider whose goals are consistent with the institution. Vendors in this space include DNS vendors such as Nominum and Bind, both of which have simple mechanisms to handle lists of banned domains.

Another solution variation is to block as much as you can with OpenDNS or utilizing an internal DNS server. By controlling DNS and thus which namespaces resolve, you can quickly disable many undesirable sites from resolving. The big caveat here is that it does not block the explicit IP itself, so users who have knowledge of the correct full IP address, can type it explicitly and be routed to the site.



3.6 Other Alternatives: Next Generation Firewalls

As stated previously, Gartner recommended that enterprises migrate from stand-alone IPS to next-generation firewalls for performing IPS functions[19]. It's unclear whether this is the future of network security, but these advanced appliances can secure both inbound and outbound communications. These devices incorporate numerous technologies such as intrusion prevention methods, network behavior analysis and firewalls. Others support additional functionality and interoperability with IPS and SIEM devices in real time.

[19] http://blogs.gartner.com/greg_young/2009/10/15/defining-the-next-generation-firewall-research-note-the-liner-notes/

3.6.1 Other Technologies in this space

- WAN (IOS) firewall solutions
- Full Proxy solutions (Smoothwall, IPCop, et al.)
- On-Ramps / ID Authentication schemes (i.e. Front Porch, Cyberoam)
- LAN/Wireless solutions (Routers such as Draytek or others that can block by packet type)

3.6.2 Target

- Larger footprints where additional security is required.
- Good for government projects or where high level security is required.

3.6.3 Vendors

Bradford Networks, Cisco, FrontPorch, Cyberoam, Cloudshield, Websense, Palo Alto Networks, Firewall vendors such as Juniper, Cisco, et al., NetEqualizer

3.7 An Integrated Approach

Real-world deployments often involve more than one technology. For example, USC and others have implemented an approach that may be viable for many colleges and universities:

- Full AAA (Authentication, Authorization and Accounting[20]) on residential, research and administrative networks

  This enables positive knowledge of *who* is at a particular network location. If portions of the institution's network are open (without authentication), this provides opportunities for infringing activities to occur without the opportunity to identify the infringer. It is likely that much of this is already deployed on campus already.

- BAYU on residential networks, with opt-out

  This turns every P2P uploading event into a teachable moment, by automatically sending information to students informing them that they may be violating school policies and putting themselves at legal risk.

- P2P blocking on wireless network.

  By blocking P2P on wireless networks, and avoiding blocking it on wired networks, this approach encourages P2P traffic onto wired ports, which can be more easily isolated to specific user(s).

- Graduated response

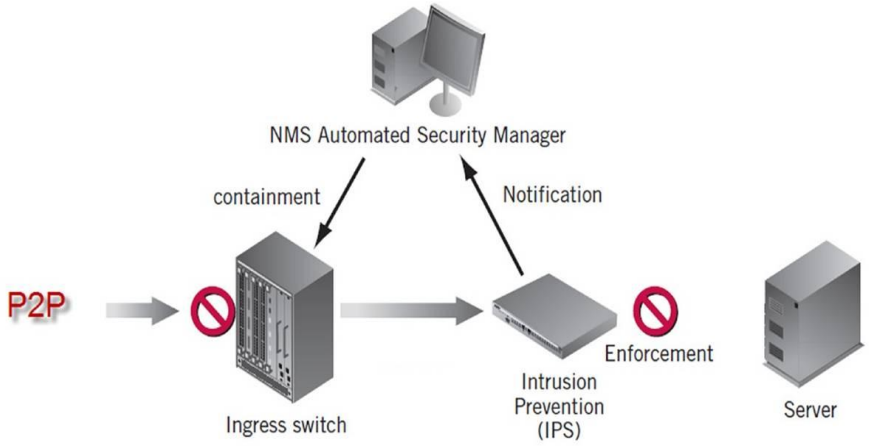
  When policy violations are found (or reported via DMCA notices), students can be explicitly informed that they've violated policies and instructed on how to avoid doing so in the future (such as making available help desk resources to remove and disable P2P applications).

[20] http://en.wikipedia.org/wiki/AAA_protocol. A common AAA protocol is RADIUS.

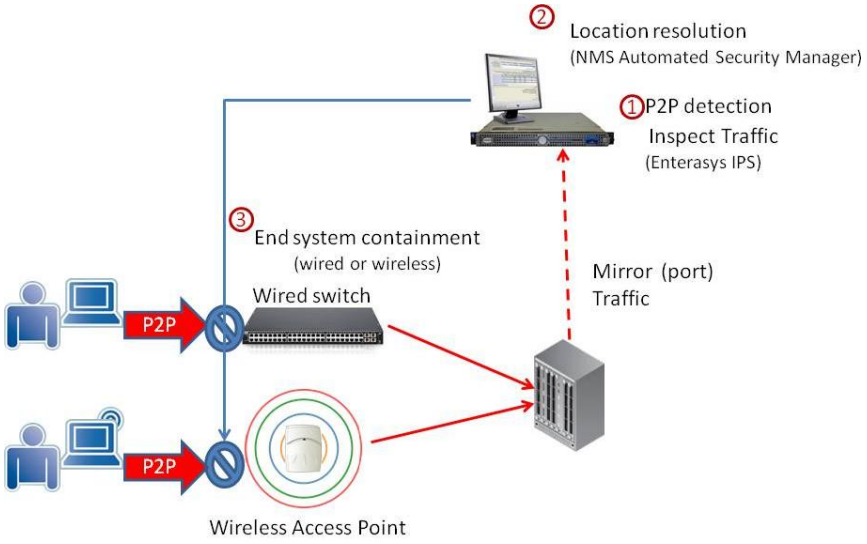
3.7.1 NAC or IPS Integrated approach using Enterasys

The diagrams on this page illustrate specific implementations leveraging the IPS system to manage P2P traffic. When unauthorized P2P traffic is detected, the user is redirected to a warning page via web intercept and informed of the potential violation. After acknowledging the warning, the user is granted Internet access. Violations are tracked and reported. After some number of violations (typically three) the user's network access can be suspended pending administrative review. The solution is implemented using a security manager working in conjunction with an IPS (e.g., Enterasys IPS) to resolve the location of the equipment in question and to enforcement policy in the infrastructure at the equipment's point of connection.

This diagram illustrates blocking of P2P at the IPS, with enforcement handled separately by the security manager controlling a user's access through the switch.

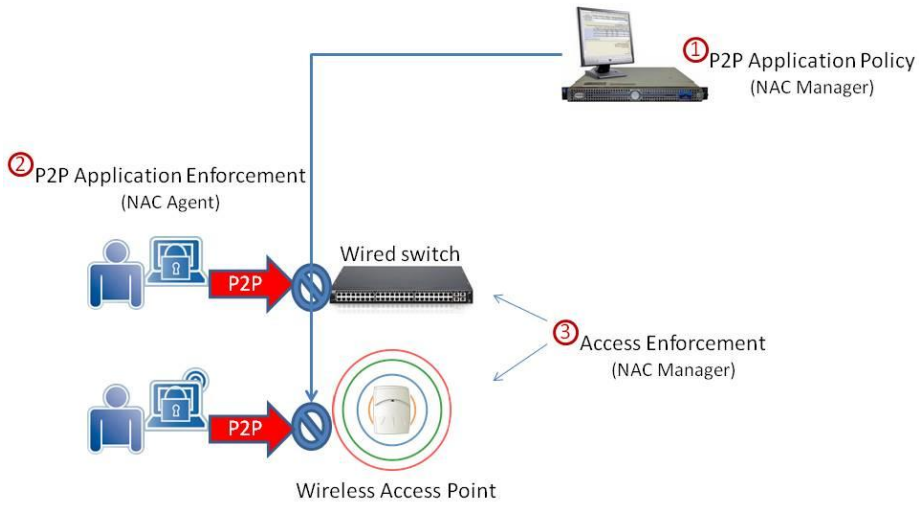


This diagram illustrates blocking P2P at the switch (i.e., without the IPS as an intermediary). It requires the security manager to take a more active role in monitoring traffic.



The diagram below is a NAC-based solution. There is a management system, called a NAC Manager that sets a policy for forbidden applications. Policies are enforced locally by the NAC agent that stops the application from executing and enforced additionally in the infrastructure.

For example, the campus could have a policy that allows the student to "opt-in" to P2P applications which disables the Access Enforcement in the WLAN/LAN infrastructure and turns off notifications in the NAC Agent.



In one deployment, UNC requires students to allow a scan of their computers before they join the campus network[21] . If the Enterasys agent software scanning their computer finds software that potentially violates policy, the student has to either remove it or sign a "hall pass" that acknowledges knowledge and responsibility for the application. The agreement includes an enumeration of the consequences of violating the policy, including a visit with the Dean. If the system detects a violation, the student is responsible. Note: a high percentage of students opt to have the software removed during the agent scan phase.

[21] http://help.unc.edu/008893

4 OTHER CAMPUS CONFIGURATIONS AND CONCERNS

Traditionally, P2P networks dominate the discussion of topics regarding illegal file sharing and copyright. This section is intended to provide background on other technologies and practices that also fall within the scope of illegal file sharing.

4.1 File sharing *within* campus

A campus network, particularly a residential network, is an excellent tool for exchanging files. Students set up servers and run programs that allow sharing directly between computers.

Illegal file sharing within a campus network presents a difficult technology problem because there is no single place to monitor this behavior and it is impractical to deploy equipment to enough places on the network to constantly monitor the entire network.

You may wish to include policies specifically addressing local file sharing in your acceptable use policies, and you may find it useful to integrate local file sharing into your graduated response program. In general, there are specific academic and/or social reasons to establish a server within a dorm that do not fall outside the bounds of wanted activities as stated by a typical campus network use policies, meaning we found much of such activity to be clearly unwanted/outside the parameters of campus network policies. With this in mind, a limited ban is worth considering. Any reasonable request can be accommodated via a waiver (for example, as is typical with BAYU and as Illinois State does with its multi-tiered approach described earlier).

4.1.1 Examples of local file sharing

It is possible for users to set up local file sharing environments without any access to the outside internet. For example, there are several "Direct Connect" software hubs and clients freely available. The Wikipedia entry has a representative list at http://en.wikipedia.org/wiki/Direct_Connect_(file_sharing).

4.1.2 Technical measures

In a large, complex, heterogeneous network it may be impractical to deploy enough equipment across a campus to constantly monitor the entire network. If you wish to monitor but don't have resources to deploy a comprehensive solution, you might consider deploying equipment on a rotating basis; randomly monitoring segments of the network (for example, a particular dorm).

4.2 Streaming and downloading from servers outside the network

Copyrighted content appears on many unauthorized sites and is available to students both as downloads and through streaming. This is challenging because many uses of downloading and streaming sites are legal, and it is difficult to differentiate such use from illegal use. For example, streaming content from netflix.com, fox.com or hulu.com would be acceptable, but downloading the same content from tudou.com (a Chinese streaming site) or rapidshare.com (a file posting/download site) would very likely be a copyright violation.

The best technical solutions for this are inline filtering options described above. You would work with the vendor to select types of sites you want blocked and they would maintain lists of such sites. This is an active area of research, development and policy, and improvements should come rapidly.

4.3 A word about Internet2 (I2), National LambdaRail (NLR) and other next-gen networks

At present, there is not enough experience with these networks and illegal file sharing to provide a definitive answer. Very high speed networks are of great concern to content owners because of the ease with which entire libraries can be exchanged.

Presumably, all the 'bad things' that happen on the Internet (spam, phishing, denial of service attacks, various forms of intrusion and illegal file sharing) will also occur on next-generation networks, and technical countermeasures for all these threats will have to be developed or adapted.

These networks are research networks, and most institutions frown upon illegal uses of expensive, scarce and valuable research tools for illegal uses.

Generally, access to advanced networks is limited. We suspect that policies with strong sanctions attached would be sufficient deterrent.

4.4 Campuses without residents or a residential networks

The responsibilities as it pertains to reducing illegal file sharing are not fundamentally different, but campuses without residents or residential networks will find the task much easier. Institutions such as community colleges that may be quite large, but with no students in residence, tend to see a smaller number of DMCA notices. Regardless, any campus with a network is likely to see some illegal file sharing and it is prudent to monitor the network. If policy-violating activities are found, then it would be necessary to adopt more proactive measures.

4.5 Institutions with limited campus networks

Some institutions are small and don't have a network accessible to students. If your institution has a small business internet connection that is only accessible to a small faculty and staff, advanced technical measures described in this document are likely unnecessary. Still, institutions should take care to avoid two common risks:

- Third parties hijacking the wireless network. Wireless networks must be secure, that is, wireless routers must use a protocol such as WAP and access to the network must require a password.
- Computers with unauthorized programs attached to the network. If someone has ever used P2P applications on personal computers (or has friends or children that have), they may inadvertently share files indefinitely (as many users are unaware of P2P programs operational characteristics). Also, malware-infected computers could be used as servers for all sorts of illegal activities. Thus it is desirable that all computers that connect to the network have anti-virus and firewall programs enabled and that all P2P programs be removed.

Policies covering good network practices should be documented or referenced in the plan, but likely no additional technical measures are required.

4.6 Outsourced technology

The technology is the same regardless of who provides the service. Please use the information in this paper in discussions with your vendors.

4.7 Managed (internally owned) assets

While this paper primarily addresses IT assets outside the direct control of a college or university, it is also necessary to consider assets owned by the institution (such as computer labs). One institution, after blocking P2P on the residential network, received DMCA notices that they subsequently traced to an administrative computer in a parking toll booth. Unfortunately, acceptable use violations are not limited to students.

As the campus has greater control over these assets, a good IT asset-management strategy coupled with endpoint protection (basic IT Service Management/ITSM)[22] should address the issue at the source, the desktop. There are many vendors providing solutions in this area, including Symantec and McAfee.

[22] http://en.wikipedia.org/wiki/IT_service_management

5 APPENDIX A. VENDOR LIST

This section provides a brief overview of vendor products applicable to combating illegal file sharing. It is not intended to be comprehensive and all product information should be verified by the vendors themselves.

The goal is to *identify* vendors. Their inclusion in this document does not constitute an endorsement.

5.1 Alcatel-Lucent

5.2 Allot Communications

Relevant URL: http://www.allot.com/Education_Solutions.html

Relevant Product Line: NetEnforcer

Category: Web filter, traffic shaping

DPI usage: Y

University References: Y (LSU, Bath, UCLA)

Description of Solution: Intelligent traffic management.

Allot NetEnforcer bandwidth management devices provide the granular visibility and policy enforcement needed to optimize the delivery, performance and profitability of WAN and broadband services. With throughput ranging from 2Mbps to 6Gbps, these flexible devices provide real-time monitoring, QoS policy enforcement and traffic steering, helping operators to control bandwidth utilization and costs while enhancing service quality for all network users. Automated, web-based update keeps the signature library up-to-date with the latest Internet developments. In a test had best obfuscated P2P detection. Integrated URL-filtering service blocks access to blacklisted and illegal web sites at the network level (via Allot WebSafe). Has integrated DDoS mitigation functionality. Centralized management console. Supports user-defined signatures based on HTTP attributes, as well as monitors reports based on custom HTTP signatures. Licensed by WAN pipe size.

5.3 Anagram (Saisei networks)

Relevant URL: http://www.anagran.com

Relevant Product Line: **Anagram Total P2P Control**

Category: P2P filtering

DPI usage: N

University References: TBS

Description of Solution: Anagram offers a device capable of P2P filtering. In addition, the solution is designed to choke out large connection types, such as torrents.

5.4 Arbor Networks

Relevant URL:http://www.arbornetworks.com/index.php?option=com_content&task=view&id=108&Itemid=69

Relevant Product Line: Ellacoya, Peakflow

Category: NBA (with AMS)

DPI usage: Y, Peakflow SP does.

University Reference: University of Michigan

Description of Solution: The Arbor Peakflow platform is an NBA, but still not focused on our target area. Focused on ISP and telcom providers, Arbor is more focused on protecting DNS and intrusion detection. Peakflow builds a model of normal network behavior. Subsequently, Peakflow alerts network operators to abnormalities or anomalies in their network traffic that could be due to simple configuration issues or new service (customer) turn-up. The Peakflow X (http://www.arbornetworks.com/en/peakflow-x.html) solution is used for internal network visibility and protection, while the Peakflow SP solution is designed for larger, carrier-class networks. In fact, Peakflow SP (http://www.arbornetworks.com/en/peakflow-sp.html) is considered by many of the world's service providers to be the de facto standard for detecting and stopping distributed denial of service (DDoS) attacks using IP flow information. By using Peakflow's flow correlation and anomaly detection capabilities, network operators can manage and secure their networks, troubleshoot and pinpoint network attacks, monitor users and applications, and report on network performance and security issues.

Primary focus is still on unauthorized malicious activity such as: scans/floods, fast spreading worms, phishing attempts, botnets, spyware and malware.

5.5 ArcSight

Relevant URL: http://www.arcsight.com/products/products-esm/

Relevant Product Line: ESM

Category: SIEM

DPI usage: N

University Reference: Weill Cornell Medical College

Description of Solution: ArcSight ESM provides the correlation infrastructure to help identify the meaning of any given event by placing it within context of who, what, where, when and why that event occurred and its impact on business risk. ArcSight ESM also correlates user entitlements to event log information and Netflow data. By quickly comparing the actions users are taking with their entitlements, analysts can instantly pinpoint privileged role violations and instances of users

performing actions outside their authorization. Will integrate to Authorization Directories (LDAP, AD).

5.6 Audible Magic

Relevant URL: http://audiblemagic.com/solutions-colleges.php

Relevant Product Line: CopySense

Category: AMS

DPI usage: Y

University References: over 120 including ASU and University of Chicago.

Description of Solution: A higher education solution with an integrated graduated response application. Audible Magic does not block or prioritize traffic but does identify copyrighted file transfers, which are tracked by user. Able to identify offenses and enable automated sanctions on a per-user basis. Can integrate into the school's user registration system via Active Directory. The CopySense Copyright Education system is a self-contained appliance and consists of integrated hardware and software running the BSD operating system. The system is a non-inline network device, which makes for easy installation and configuration, as has no impact on network reliability or performance.

All functions are managed via an easy-to-use web browser interface. The CopySense Appliance is remotely maintainable with system software upgradeable over HTTP. The system identifies copyrighted content via a database service. System protects privacy by restricting information on usage to the student violator.

UPDATE (version 2.0):

- AudibleMagic had added DMCA notice administration to the appliance.
- Incorporated a peer capability within the box to detect the presence of copyrighted content when communications is encrypted P2P.

5.7 Barracuda

Relevant URL:
http://www.barracudanetworks.com/ns/products/purewire_web_security_service_overview.php

http://www.barracudanetworks.com/ns/downloads/White_Papers/Barracuda_Web_Filter_WP_Web_Access_Educational_Institutions.pdf

Relevant Product Line: Purewire

Category: Firewall or cloud-based web-filter (via proxy)

DPI usage: Y

University References: Harvard

Description of Solution: The Barracuda Purewire Web Security Service, a SaaS-based secure Web gateway, protects users from malware, phishing, identity theft and other harmful activity online, providing a "clean" Internet. The service sits between an organization's network and the Internet to protect users as they conduct business-critical activities on the Web.

5.8 BAYU

Vendor: BAYU (Be Aware You're Uploading)

Relevant URL: http://bayu.umich.edu, http://bayu.umich.edu/guide/about.php (Last modified: November 02 2011.)

Relevant Product Line: BAYU software

Category: Software Based AMS (Build your own traffic shaper)

DPI usage: N

University References: University of Michigan (also the author), USC, Northwestern

Description of Solution: BAYU is popular option because it is publicly available, relatively easy to implement, and does most operations without direct involvement of campus administrators.

Every 10 minutes BAYU receives data from a device such as a PacketShaper that detects protocol usage, and uses software to determine whether actions should be taken on that detection. The service maps IP addresses used for P2P exchange to a corresponding MAC address, and it uses existing housing registration databases to map the MAC address to a user's ID. The service records IP addresses that it is unable to map, so they can be resolved manually. The service sends a BAYU notification message to the user in question at their campus e-mail address and will do so once every 24 hours (configurable) while the usage continues. It records failed delivery attempts, so they can be resolved manually. If students are using P2P legitimately and they don't wish to receive the reminder, they can opt out.

5.9 Bluecoat

Relevant URL: http://www.bluecoat.com/solutions/industry/higher-education

Relevant Product Line: PacketShaper

Category: Firewall, DPI

DPI usage: Y (Packetshaper)

University Reference: Carroll University, Student Housing at University of California

Description of Solution: Available in both appliance and cloud based solutions, ProxySG allows for activity visibility and priority delivery of educational traffic, including P2P, torrents, etc.Bluecoat claims to be implemented at over 1000 universities world-wide.

5.10 Bradford Networks

Relevant URL: http://www.bradfordnetworks.com/education

Relevant Product Line: Campus Manager and Rogue Tracker

Category: Firewall, Response to events detected elsewhere

DPI usage: Y

University Reference: Bryant (http://www.bradfordnetworks.com/4696)

Description of Solution: Campus Manager is part of an overall solution. It is particularly useful in responding to events detected through SIEM, AMS or IDS. In particular, Campus Manager can be used to isolate an endpoint found to be violating policy. It can be used as part of a graduated response system.

Campus Manager automatically identifies authorized users and verifies security policy compliance of endpoint devices before granting network access. If users fail to gain access, Campus Manager provides remediation options so non-compliant users can update their systems themselves. Campus Manager then continuously enforces security policies, records detailed historical data to document network activity, and generates reports for security threat analysis and regulatory compliance. This is a location and device tracking solution.

Bradford has expanded into including NAC based solutions.

5.11 Cisco

Relevant URL: http://www.cisco.com/en/US/products/ps6120/index.html

Relevant Product Line: ASA, IronPort and SCE, (TrustSec and ISE), NBAR

Category: Firewall, IDS, bandwidth shaping respectively

DPI usage: Yes and more

University References: unexplored

Description of Solution: The Cisco ASA 5505 Adaptive Security Appliance is a next-generation, full-featured security appliance for small business, branch office, and enterprise teleworker environments. The Cisco ASA 5505 delivers high-performance firewall, SSL and IPsec VPN, and rich networking services in a modular, "plug-and-play" appliance.

The Cisco IronPort Web Security Appliance is a secure web gateway that combines acceptable-use-policy (AUP) controls, reputation filtering, malware filtering, data security, and application visibility and control on a single platform. The Cisco IronPort S-Series helps organizations address the growing challenges of both securing and controlling web traffic whether their employees are tethered to a corporate LAN or sitting in an airport on their smart-phones.

Cisco SCE (Service Control Engine) provides ability to shape or block traffic. Their EasyApp can offer a "Safe Internet Experience" by blocking unsuitable sites. H. This offers value to a campus with the ability to block specific URLs used for illegal downloads. (It can be as broad as a site, or specific as a download file location.)

Cisco is also improving Identity Services, to unsure unauthorized users and traffic cannot utilize a network (ISE-based TrustSec LAN Deployment). NAC (Network Access Control) solutions are becoming more viable and popular choices. A NAC based solution controls the on-ramp process and as the user connects to the network, they are met with additional criteria that must be met in order to access resources. This may involve as little as a acceptance of an "Acceptable Use Policy" to a more invasive scan of the machine or even the installation of a monitoring agent.

For Cisco based router networks, there is an additional tools called in the IOS. Network-Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate quality of service (QoS) for that application or traffic with that protocol. The QoS settings can slow down or even discard suspect packets.

http://www.cisco.com/en/US/products/ps5855/products_configuration_example09186a0080ac3082.shtml#backinfo

5.12 Cloudshield

Relevant URL: http://www.cloudshield.com/applications/cs_tcss.asp

Relevant Product Line: Traffic Control and Security Solution (TCSS)

Category: Inline traffic shaper

DPI usage: Y

University References: N

Description of Solution: This is essentially a traffic shaper, although it offers other capabilities such as DDoS protection.

5.13 Cyberoam

Relevant URL: http://www.cyberoam.com/

Relevant Product Line: Unified Threat Management

Category: Advanced Firewall/IDS

DPI usage: Y, depending on application

University References: Yes. Their web site has case studies in India and Turkey.http://www.cyberoam.com/cyberoam/jsp/whitepapers/resources.jsp

Description of Solution: Cyberoam takes the perspective of identity-based policy control; that is, know who is on the network, detect whether there is inappropriate activity and respond directly to the system/person creating the security incident. Their appliance offers both firewall and IPS functionality, so it is looking both inside the network and outside. Their UTM solution is doing URL-based content filtering which is a needed capability for fully addressing campus piracy. Control is at the granularity of users or groups of users. QoS, along the lines of traffic shaping, can be applied. (IP6 ready)

5.14 Endace

Relevant URL: http://www.endace.com/endace-security-manager.html

Relevant Product Line: Cyber Security Monitoring

Category: Monitoring; IDS (when used with Snort)

DPI usage: N (Y, when used with Snort)

University References: N

Description of Solution: Their emphasis is very high speed monitoring. They can be a Netflow source and can integrate with Snort to produce an IDS solution. Possibly applicable to high-speed links (10Gbps+).

5.15 Enterasys

Relevant URL: http://www.enterasys.com/solutions/HigherEducation.aspx and

http://www.enterasys.com/company/literature/controlling-P2P-traffic-sb.pdf

Relevant Product Line: "Solutions for Higher Education"

Category: SIEM w/NBA + IDS/IPS + **NAC** support

DPI usage: Y

University References: 32+

Description of Solution: Enterasys has solutions that provide visibility, control, and action-oriented prevention to help those responsible for IT in university environments move from being reactive to proactive. A Security Information and Event Manager (SIEM) solution combines best-of-breed detection methodologies with behavioral analysis and information from third-party vulnerability assessment tools. The suite delivers threat management, log management, and compliance reporting, and claims increased operational efficiency. The console delivers actionable information to effectively manage the security posture for challenging environments such as colleges and universities. (IP6 ready)

Bentley College uses the Enterasys IPS function as a detection mechanism and the Automated Security Manager to perform network isolation of the offending system. The offending traffic

matches a signature or rule in the IPS, the IPS sends the event information to Enterasys Automated Security Manager (ASM), and ASM matches the event to a preset action such as: "locate" the offender system, "modify" the network access privileges for the offending system. The result is "eliminating" the offense (P2P, virus, worm) and "informing" the end user via remediation system (such as web page redirect).

Enterasys can also combine Audible Magic with the Automated Security Manager to perform isolation on any network vendor's managed switch or wireless infrastructure.

The University of North Carolina at Chapel Hill (UNC-CH) has leveraged the Enterasys NAC product, with remediation available via web or agent, to monitor for known P2P programs and inform the user that running this program potentially violates UNC-CH code of conduct etc. The agent also offers the ability to block the program from running although UNC-CH offers the ability to "opt out" by signing a waiver of responsibility. This opt-out act would then place that user's system in a policy group that disables the blocking function of the agent.

5.16 Facetime

Relevant URL: http://www3.facetime.com/productservices/prodservices.aspx

Relevant Product Line: Unified Security Gateway

Category: Web filter or as an add-on product to a web filter.

DPI usage: Y

University References: Eastern Kentucky
Description of Solution: USG provides granular control of not only Web sites and applications but also the content posted to blogs, wikis, webmail, Instant Messaging and social networking sites. Content posted to these social networks can be moderated, monitored and logged – reducing outbound data leakage and enabling compliance, legal-discovery requirements, and corporate-policy standards. Granular controls for Facebook, LinkedIn, Skype and Twitter, including monitoring, moderation, and archiving.

5.17 FrontPorch

Relevant URL: http://www.frontporch.com/

Relevant Product Line: FPS

Category: Authentication and Messaging

DPI usage: N

University References: Y

Description of Solution: A suite of solutions for Internet providers offers a scalable, reliable option for messaging Internet subscribers. The PorchLight™ appliance coupled with the central web-based Front Porch Services (FPS) management system enable providers to communicate directly to the

subscriber through their Internet browser, regardless of Internet platform, browser or operating system, without the need for client software or configuration. They integrate with RADIUS and other AAA systems.

FrontPorch is used widely in wireless networks (for example, in airports) to control and track access. As accountability on wireless networks is important to avoiding illegal behavior, FrontPorch systems can provide login services. They also offer solutions to intercept traffic to sanctioned users and require some action. This is ideal for students to acknowledge a violation and to receive educational services.

In the case of violation, Front Porch software is informed and the next time the user tries to access the web, he or she is redirected to the appropriate site. If used inline, then non-browser traffic can be redirected and then the user is forced to respond before accessing the Internet.

New focus on marketing messaging and bandwidth consumption.

5.18 HP

Relevant URL: http://www.tippingpoint.com/products_ips.html

Relevant Product Line: TippingPoint

Category: IPS

DPI usage: Y

University References: Illinois State University, TBD

Description of Solution: In addition to general IPS capabilities, TippingPoint can block P2P.

TippingPoint's Intrusion Prevention Systems provide application, performance, and infrastructure protection via total-packet inspection. Application Protection capabilities provide fast, accurate, reliable protection from internal and external cyber attacks. TippingPoint IPS protects VoIP infrastructure, routers, switches, DNS and other critical infrastructure from targeted attacks and traffic anomalies. TippingPoint's Performance Protection capabilities enable customers to throttle non-mission-critical applications that hijack valuable bandwidth and IT resources, thereby aligning network resources and business-critical application performance.

The system is built upon TippingPoint's Threat Suppression Engine (TSE) - a specialized hardware-based intrusion prevention platform.

5.19 IM Firewall

Relevant URL: http://www.imfirewall.com/en/education-network-monitor-solution.htm, http://www.imfirewall.us/installGuide_http.htm

Relevant Product Line: WFilter

Category: Web filter

DPI usage: Y

University References: N

Description of Solution: A software based AMS. WFilter is an Internet filtering software solution that can help organizations monitor and manage all Internet behaviors on their networks. It claims to be able to block both P2P and selected sites. WFilter can detect and block p2p traffics by pattern match. It can pick up a p2p connection by packet analysis and block it.

5.20 Internet Systems Consortium (BIND)

Relevant URL: http://www.isc.org

Relevant Product Line: BIND

Category: DNS

DPI usage: N

University References: (very widely used)

Description of Solution: The free DNS provider has added the ability to block sites using their RPZ functionality.

5.21 ipoque

Relevant URL: http://www.ipoque.com/solutions/education

Relevant Product Line: Traffic Manager

Category: web filter (focus on bandwidth management and whitelisting)

DPI usage: Y

University References: German

Description of Solution: PRX Traffic Manager is a solution enabling network operators to monitor and control network traffic per application and per subscriber. PRX Traffic Manager detects applications with a combination of layer-7 deep packet inspection (DPI) and behavioral traffic analysis. All major protocols including peer-to-peer file sharing (P2P), instant messaging (IM), media streaming and Internet telephony (VoIP) are supported. The integrated quality-of-service (QoS) management allows prioritization, shaping and blocking of classified traffic. Extensive accounting features provide in-depth application and network visibility.

5.22 Irdeto Intelligence (formerly BayTSP)

Relevant URL: http://irdeto.com/en/anti-piracy-services.html

Relevant Product Line: Business Intelligence and Monitoring Services

Category: AMS

DPI usage: N

Irdeto offers a non-intrusive program designed to assess and support compliance with the new Federal requirements for technology-based deterrents. These programs are designed to provide measurement of pre- and post-implementation of the required policies and technical-based deterrents to unauthorized distribution of copyrighted materials on universities' networks. Note that Irdeto has the ability to monitor external activity, particularly P2P, so campuses can have some measure of the volume of P2P-related notices they will be receiving.

In their words: *Irdeto has designed a two Phase Program.*

1. ***Initial Assessment and Consulting*** *– Irdeto would provide an initial assessment of the current University's Internet Copyright Policy and Procedures to determine if the controls in place meet the HEOA compliance requirements.*
2. ***Program Monitoring*** *– Irdeto will work with the University on implementing a program to measure the performance of its policies and support systems to reduce the unauthorized distribution of copyrighted material on its networks to measure the impact of its policies and systems.*

5.23 Juniper

Relevant URL: http://www.juniper.net/us/en/solutions/public-sector/research-education/colleges-universities/

Relevant Product Line: Intrusion Detection and Protection (IDP), Integrated Security Gateway (ISG), Netscreen, Secure Service Gateway (SSG), Unified Access Control (IC)

Category: Firewall, IDS, Network Access Control

DPI usage:

University References: Y

Description of Solution: Juniper Networks provides a diverse set of solutions that help educational institutions communicate and share more effectively through the provision of carrier-class routing platforms, network security and access systems with firewall, IPsec and SSL VPNs, and intrusion detection and prevention technologies that ensure the dependability and security of their networks.

5.24 Lancope

Relevant URL: http://www.lancope.com/industries/higher-education/

Relevant Product Line: StealthWatch

Category: SIEM with NBA, IDS/IPS

DPI usage: Optional

University References: Grafisch Lyceum Rotterdam, Darmouth, Yale.

Description of Solution:

Lancope utilizes NetFlow Collection & Analysis for flow-based network performance and security monitoring under the general category of Network Behavior Analysis. A Lancope system when deployed could be integrated with a system such as Bradford Networks or FrontPorch to respond to the violation.

A supporter of the EDUCAUSE Identity Management Services Program (IMSP), Lancope helps academic institutions protect their networks and enhance network and security operations with preferred member pricing for Lancope's identity tracking solution the StealthWatch IDentity appliance, a component of the StealthWatch System.

V6.2 adds functional improvements to identification and additional NAT support in upcoming v6.3 release. Now with integration with Cisco ISE solution (part of TrustSec* platform). Utilizes known bot-net lists to insure machines not communicating with known malware machines.

**Cisco TrustSec integrates with the CiscoSecureX architecture to allow the Cisco security portfolio to use network-based identity context for full context-aware firewalling and policy enforcement.*

Can be purchased as both appliance or virtual machine form factor.

5.25 LogLogic

Relevant URL: http://www.loglogic.com/products

Relevant Product Line: SEM

Category: SIEM

DPI usage: N

University References: N

Description of Solution: Log and event management reporting tool. Focused mainly on Compliance and compliance management.

5.26 NetEqualizer

Relevant URL: http://www.netequalizer.com/nda.htm

Relevant Product Line: NetEqualizer

Category: Bridge Router

DPI usage: Y

University References: Specifically claims to be a HEOA technology deterrent.

Description of Solution: NetEqualizer appliances are bandwidth-shaping appliances, designed for voice and data networks. The bandwidth-control products can be deployed in both corporate and

service provider networks. They claim 'behavior-based control and containment of all common encrypted and unencrypted Peer-to-Peer (P2P) Applications.'

5.27 Nominum

Relevant URL: http://www.nominum.com

Relevant Product Line: Vantio

Category: DNS

DPI usage: N

University References: Penn State (as per press release)

Description of Solution: Nominum is a DNS vendor who provides DNS servers have a redirection tool that can easily be added to their products.

5.28 Palo Alto Networks

Relevant URL: http://www.paloaltonetworks.com/solutions/threats.html

Relevant Product Line: Threat Prevention

Category: Next Generation Firewall

DPI usage: Y

University References: TBD

Description of Solution: Firewalls with integrated IPS. Added Malware defense to their firewalls via their new WildFire technology.

5.29 Procera

Relevant URL: http://www.proceranetworks.com/en/solutions/higher-education.html

Relevant Product Line:

PacketLogic Smart Campus – A Turnkey Traffic Management Solution for Higher-Education Institutions

Category: Switches and Router Hardware combined with analysis server software for subscriber awareness and analysis.

DPI usage: Y (possibly just protocol)

University References: TBD

Description of Solution: Hardware based Filtering, Traffic Shaping and Statistics.

5.30 Q1 Labs

Relevant URL: http://q1labs.com/

Relevant Product Line: Q1 Radar

Category: Next Generation SIEM

DPI usage: Y

University References: Y, Texas A&M

Description of Solution: QRadar's network activity collection and analysis provides comprehensive security capabilities beyond simple log collection, resulting in an improved ability to detect and remediate threats, enforce network policies and minimize risk to mission-critical IT systems.

5.31 Red Lambda

Relevant URL: http://www.redlambda.com/products/metagrid

Relevant Product Line: MetaGrid (formerly Integrity)

Category: IDS

DPI usage: Yes, but not data.

University References: Yes. MetaGrid (formerly Integrity) is based on a technology originally developed at the University of Florida.

Description of Solution: Red Lambda's approach is based on the use of many inexpensive computers across a campus network. MetaGrid shares information between nodes to create a better picture of network activity, increasing the effectiveness of detection. It is an out-of-band solution, utilizing SPAN/monitor ports on switches. This product can identify the real user with access to the AAA or RADIUS server—not all products in this category can. MetaGrid supports RADIUS and LDAP connections out-of-the-box. NAC integration is available. Grid Platform allows any idle computers to participate in the processing, saving the cost of a high-end server.

MetaGrid is identity-aware and can identify and enforces compliance policies. When combined with workflow and case management capabilities, the Integrity P2P Control VGA provides an automated approach to managing the network behavior of employees, students, and subscribers, enforcing authorized use policies, and responding to compliance notifications.

5.32 Riverbed

Relevant URL: http://www.riverbed.com/results/

Relevant Product Line: Steelhead

Category: WAN Optimization

DPI usage: N

University References: None specific to HEOA

Description of Solution: Has a deep layer of visibility and analytics. Note that Riverbed acquired Mazu networks along with their product line.

5.33 RSA

Relevant URL: http://www.emc.com/security/rsa-identity-and-access-management/rsa-access-manager.htm

Relevant Product Line: Access Manager

Category: Authentication and control

DPI usage: N

University References: unexplored

Description of Solution: Access Manager enables organizations to manage authentication and authorization policies for a large numbers of users from a central location. This ensures that only authorized users can access sensitive data within web-based applications, ensuring that the right people have the right access at the right time. Access privileges can be determined by select attributes, such as function and responsibilities, and can be readily turned off if a person departs.

5.34 Sandvine

Relevant URL: http://www.sandvine.com/products/traffic_management.asp

Relevant Product Line: Policy Traffic Switch

Category: Hardware Switch

DPI usage: Y

University References: N

Description of Solution: Allows service providers to optimize bandwidth usage per subscriber. Here is a paper Sandvine wrote in response to a Higher Education RFI: http://net.educause.edu/Elements/Attachments/rfi/vendors/sandvine.pdf.

5.35 SenSage

Relevant URL: http://www.sensage.com/content/advanced-siem-and-log-management

Relevant Product Line: Event Data Warehouse

Category: SIEM

DPI usage: N

University References: N

Description of Solution: A data warehouse approach to SIEM emphasizing long term analysis.

5.36 Skybox

Relevant URL: http://www.skyboxsecurity.com/

Relevant Product Line: Threat Manager

Category: Firewall + SIEM

DPI usage: N

University References: N

Description of Solution: Skybox Threat Manager can centrally manage threats from disparate sources, analyze threats in a timely manner, and initiate steps to remediate. Threat Manager easily manages threat workflow by continuously presenting the latest update of an alert, highlighting matches in the system, and executing queries that automatically prioritize vital threats to the organization. A firewall (+SIEM) that takes feeds from Symantec and VeriSign to halt unwanted traffic and destinations. New Focus on Financial solutions

5.37 Snort

Relevant URL: http://www.snort.org

Relevant Product Line: Snort

Categories: SIEM (as sniffer), IDS/IPS

DPI usage: Y

University References: Snort has been on campus both as an administrative tool and a teaching tool.

Description of Solution: Snort is popular free open-source network intrusion detection/prevention system. It can be configured as a sniffer, packet logger or IDPS. Other open-source projects have been created based on Snort. Snort can also be used to monitor other solutions or just to assess the status of activities on campus. The advantage is complete control. The disadvantage is the need to fully manage a deployment.

5.38 St Bernard (EdgeWave)

Relevant URL: http://www.edgewave.com/

Relevant Product Line: iPrism

Category: web filter

DPI usage: Y

University References: TBD

Description of Solution: An appliance-based solution. iPrism delivers Internet security at the perimeter, to help enforce Internet-acceptable use and security policies. iPrism integrates with your directory services to automate authentication. A new Hybrid Remote Filtering assures policy

enforcement for all on-premises or remote employees without using VPN or DMZ deployments. Simple to set up and requiring virtually zero maintenance, the iPrism Web Filter allows your organization to mitigate the risks of legal liability, defend against security breaches, and prevent productivity loss. Focus on Acceptable Use Policy

5.39 Tenable

Relevant URL: http://www.tenablesecurity.com/products/sc/

Relevant Product Line: Network Security Nessus

Category: SIEM + AMS

DPI usage: N

University References: N

Description of Solution: More of an asset management system, it guards endpoints against myriad issues.

5.40 Websense

Relevant URL: http://www.websense.com/content/WebSecurityOverview.aspx

Relevant Product Line: Web Security

Category: Firewall + Web filter

DPI usage: Y

University References: TBD

Description of Solution: A high end solution, Websense web security is focused on malware protection, site blocking, and data loss (IP) prevention. Now offering a SaaS version. Websense has been used effectively to block download sites and is considered a leader in this area.

5.41 Others

Other companies have offerings in this area. We regret not having the opportunity to include more. We hope to revise this paper periodically and include additional offerings.

In 2008, the Joint Committee of Higher Education and Entertainment Communities conducted a RFI for vendors in this area, and the responses are here: http://www.educause.edu/EDUCAUSE+Major+Initiatives/JointCommitteeoftheHigherEduca/1204. Some of the respondents are included in this report and some are not (as a matter of time, rather than of merit).

6 APPENDIX B. THE HIGHER EDUCATION OPPORTUNITIES ACT (HEOA)

Provisions of the *Higher Education Opportunity Act of 2008* obligate higher education institutions to take measures to combat the unauthorized distribution of copyrighted material. Broadly, these measures[23] are:

- An annual disclosure to students describing copyright law and campus policies related to violating copyright law.
- A plan to "effectively combat the unauthorized distribution of copyrighted materials" by users of its network, including "the use of one or more technology-based deterrents."
- A plan to "offer alternatives to illegal downloading."

Information in this document is aimed at campus CIOs and CTOs tasked with considering options for "technology-based deterrents," four categories of which are defined by the Department of Education:

1. Bandwidth shaping
2. Traffic monitoring to identify the largest bandwidth users
3. A vigorous program of accepting and responding to Digital Millennium Copyright Act (DMCA) notices
4. A variety of commercial products designed to reduce or block illegal file sharing

These categories are equally valid in meeting the requirement to use one or more technology-based deterrents.

[23] Taken from: http://www-cdn.educause.edu/Resources/Browse/HEOA/34600

7 APPENDIX C. EVOLVING TECHNOLOGIES USED FOR ILLEGAL FILE SHARING

Illegal file-sharing technologies continue to evolve, and so must techniques to mitigate illegal sharing. Fortunately, many of the products discussed here, such as intrusion prevention systems, are designed to adapt to changing conditions. One must realistically expect that reducing illegal file sharing is an ongoing activity.

We have found that downloads directly from file servers (for example, cyberlockers) have increased substantially. Streaming copyrighted material without authorization directly from servers has also increased. Darknets (networks, often built in the Internet, whose behavior is not directly observable), VPNs and proxy servers have all been used to hide behavior. High-speed research networks such as Internet2[24] and National LambdaRail[25] have the potential to be used for illegal activities.

Some technologies, such as ID management and authentication offer solutions in both the near and long term. For example, requiring people to register computers that access campus resources will continue to be a valuable tool. Campuses often require a malware scan prior to registration. The use of this technology can be used to inform students their computer is running illegal file sharing tools.[26] As the file sharing tools change, so will the scanning software.

Following are some examples of illegal file sharing technologies you might see on campus.

7.1 Illegal file sharing technologies

7.1.1 P2P (peer-to-peer)

A substantial portion of the illegal file sharing is currently taking place using these protocols (BitTorrent[27]; eDonkey2000/ED2K, Kademlia/KAD, FastTrack, Gnutella, among them). P2P applications perform the actual file sharing itself through the use of an index file (aka the .torrent file) which tells the application which site is hosting the indexed list of dynamic download peers for a given file share. Those peers are then fed back to the program and blocks of files are then exchanged via direct peer-to-peer transfers. P2P networks work, even if there are no servers that serve up the file.

Torrent sites[28] like thepiratebay.com, torrentz.com, isoHunt.com facilitate illegal file sharing by posting "torrent" files used for P2P file sharing. Torrent files are typically published and registered with at least one tracker. The tracker maintains lists of the clients currently participating in the torrent. Newer technologies such as distributed hash tables (DHT) and peer exchange (PEX) allows P2P networks to operate without trackers.

[24] http://www.internet2.edu
[25] www.nlr.net
[26] The University of North Carolina recently initiated network access control to confirm users' identities and be able to warn students if potentially malicious software was on their pc.
http://www.dailytarheel.com/index.php/article/2011/01/scan_to_notify_illegal_sharers
[27] http://en.wikipedia.org/wiki/BitTorrent_%28protocol%29
[28] http://en.wikipedia.org/wiki/Comparison_of_BitTorrent_sites, http://www.slyck.com/bt.php?page=3

What we found is that most students do not realize is that it's almost impossible to download without uploading. Furthermore, once a file is downloaded, the P2P application will upload the file until told to stop. As applications load at boot, this may persist as a computer is moved from home to school and beyond.

P2P has been the focus of most anti-file sharing attention and consequently there is a broad range of technical solutions available to campuses.

7.1.2 Darknet

The term 'darknet' is used to refer to a variety of different technologies that hide or obfuscate user behavior. Generally darknets are built on the Internet, but have their own addressing and routing. Darknets may take the form of virtual private networks (VPNs), servers not listed in DNS, or specialized networks such as Tor (The Onion Router).[29]

It is, in effect a network within a network with private users. Darknets are used to hide illegal behavior, including illegal file sharing. Darknets external to campus networks provide some challenge to anti-file-sharing technology, although their limitations slow their adoption.

Darknets on campus provide a challenge to detecting illegal file sharing on campus networks, especially if they are localized. Deploying monitoring equipment with adequate coverage is often impractical, and a more policy-based approach is required (including disciplinary consequences for operating a darknet).

7.1.3 File sharing lockers/Cyber lockers (Rapidshare, et al)

These sites allow users to store large files in the "cloud." These services not only include virtual lockers like Rapidshare[30], but also file back-up sites that allow multiple-user access. Even Microsoft (via Live) offers such a repository and they are becoming commonplace. Most cyberlockers do not include the facility to search contents. Consequently, blog sites and other servers (such as filestube.com) may provide easy links to cyberlockers.

Although some sites are so predominantly used for illegal activities that it often makes sense to block those sites completely, technologies exist to block specific URLs referring to verified illegal postings.

7.1.4 Rent, Rip and Return

DVDs and Blu-rays are available via subscription (through, for example, Netflix) rent (RedBox and others) or purchase through a variety of sources. Tools, often in violation of the DMCA, allow simple copying or "ripping" of these discs to storage media (hard drive, flash, and so on).

Although most Rent, Rip and Return is outside the purview of campus administration, some policies might apply, such as not allowing ripping applications on campus-owned machines and informing students who borrow media from campus libraries that retaining a copy is not allowed.

[29] http://www.torproject.org/
[30] http://www.rapidshare.com/

Files obtained in this manner are often shared or hosted, possibly on IT servers online utilizing campus resources. Massive file usage is often an indication of large caches of video material. Student-operated servers with massive storage are often an indication of media distribution.

7.1.5 Sneaker-net of unprotected files (trading files)

Anyone with digital content can trade that content through the use of external storage such as USB-based flash drive swapped in-person. A terabyte external drive can hold the collective music library of a dorm, or hundreds of movies. These files are usually obtained from the Internet.

Where campus resources are used, these activities should be prohibited. On the broader issue, campuses may wish to work this into their education policy.

7.1.6 Newsgroups and NZB files

Newsgroups (aka Usenet groups) can host binary files despite being originally intended for discussions. This is done through a complex conversation (Uuencode[31] and later on Base64[32] and yEnc[33]), which posted the binary in digestible chunks directly in messages. In response to the demand, independent newsgroup hosting sites have sprung up to support this type of file hosting. However, large files must be broken into pieces to conform to limits on maximum message size. In order to facilitate the locating of the desired file pieces to facilitate their reassembly, NZB files were developed. These contain the relevant newsgroup(s) and the exact message numbers needed to reconstruct the given file(s).

7.1.7 Pay Per View copying

This is transfer of a digital transmission intended for a single person, to a redistributable binary file. An example is downloading a Pay-per-view event to a hard-drive via some capture technology.

[31] http://en.wikipedia.org/wiki/Uuencode
[32] http://en.wikipedia.org/wiki/Base64
[33] http://en.wikipedia.org/wiki/YEnc

8 APPENDIX D. GLOSSARY

8.1.1 DPI (Deep Packet Inspection)

The term Deep Packet Inspection (DPI) is broad term covering a range of technologies and uses. A common misconception is that DPI inherently looks at content. Most DPI systems only look at protocol information, not the data itself. As it is such a broad term, it is essential to understand the specific underlying technology before reaching a conclusion regarding the suitability of DPI in any given application or environment.

Generally speaking, DPI is the act of looking beyond the headers of a network packet and examining some other data in a packet. In some cases, 'data' would be application protocol headers (identifying the protocol), and in other cases 'data' might be the actual content (such as a song).

DPI has been used for years to determine traffic shaping and Quality of Service allocations for applications by Internet Service Providers. In all likelihood, you have intrusion protection systems (IPSs), traffic shapers, statistics gathering tools or spam filters that are using DPI. Aside from the legal issues, colleges and universities may have a philosophical apprehension concerning DPI. For that reason, where and how DPI is used will be referenced in the vendor list. Most web-filtering technologies utilize this technology to determine packet and application types.

8.1.2 Flow Analysis

NetFlow[34] is a protocol developed by Enterasys Networks[35] and Cisco Systems[36] for collecting IP traffic information. It is proprietary, but is supported by platforms other than Cisco IOS such as Juniper[37] routers. Other vendors have alternatives, such as NetStream, sFlow, Rflow and Jflow.

NetFlow data is exported by switches and routers and aggregated to a database that can parse and analyze the data.

In the current generations of Cisco ASA products, security event logging is included in the NetFlow data. In addition, more and more switches are making the NetFlow data available via monitored link (or mirror) port so that there is no impact on traffic flow from the monitor.

8.1.3 Authentication, Authorization and Accounting (AAA)

AAA systems allow administrators to authenticate users, authorize access to particular networks or functions, and account for their behavior.

AAA is essential to identifying Acceptable Use Policy violators and controlling their access. When a violation occurs, it is necessary to know who the violator is and where on the network the violation occurred, and subsequently to have the ability to limit access. Generally, it is necessary at all times to be able to map an IP address and port to a given student. If NAT (Network Address

[34] http://en.wikipedia.org/wiki/Network_protocol, http://en.wikipedia.org/wiki/Netflow
[35] http://www.enterasys.com/, http://en.wikipedia.org/wiki/Enterasys_Networks
[36] http://www.cisco.com, http://en.wikipedia.org/wiki/Cisco_Systems
[37] http://www.juniper.net, http://en.wikipedia.org/wiki/Juniper_Networks

Translation) is used, then it must be possible to determine who was using a particular port at a given time.

Some campuses have opted to offer limited access (for example, P2P blocked) on wireless networks where they can't control access. This is an acceptable solution, but the better option is to control access to the wireless network.

The most common AAA protocol is RADIUS. RADIUS (or Remote Authentication Dial In User Service) provides centralized AAA management for connecting computers to a network LAN or service. Although "dial in" is part of the acronym, any remote connection now applies (such as VPN). In solutions that act upon the user's access or account information, the solutions are almost always designed to work with a RADIUS server.

8.1.4 ACNS

ACNS stands for Automated Copyright Notice System and details can be found at http://www.acns.net. Likely, every notice received on campus contains XML conforming to the ACNS spec that is computer-readable and designed to automate notice processing. It's an open source, royalty-free specification that colleges and universities, ISPs, or anyone that handles copyright notices can implement on their network to increase the efficiency and reduce the costs of handling the notices.

The system is a flexible design that can be implemented on just about any network, using already available network equipment such as routers and packet shapers. It is not intrusive and does not invade the privacy of the networks users, and it lets the university or ISP enforce its own policies with regard to network abuse and copyright infringement. It has features added at the bequest of Higher Education to facilitate tracking of notices within a campus.

ACNS provides the opportunity to automate the process of DMCA notice handling. The more automated this process is, the better chance the notice reaches the student in a timely fashion. Notices received promptly have the most impact.

8.1.5 Escalated/Graduated response

Sometimes known as "three strikes", this is an approach aimed at addressing online copyright infringement. In response to copyright infringement (such as using peer to peer software) many content providers advocate what is known as a "graduated response." This response has increasing levels of consequence subsequent to receipt of notification letters or messages warning that they are in violation of copyright law.

With graduated response, the college or university is either processing an internal Terms of Use violation (possibly using techniques described here) or is acting on a notice sent to the campus, typically a DMCA or other form of informational notice. The first violation typically results in an acknowledgement from the student along with some educational activity. The student is given sufficient information to prevent subsequent violations including information or assistance how to remove violating programs from their computers (if applicable).[38]

[38] Here is an example of a page providing information on removing P2P applications. http://itservices.uchicago.edu/services/safecomputing/disableptp/

If violations continue, the responses will includes increasing severe consequences. They may include the temporary limitation or suspension of services and campus disciplinary actions. Campus administrators have reported that an appointment with the Dean or risk of a notation on a student's permanent record is particularly effective in deterring subsequent violations.

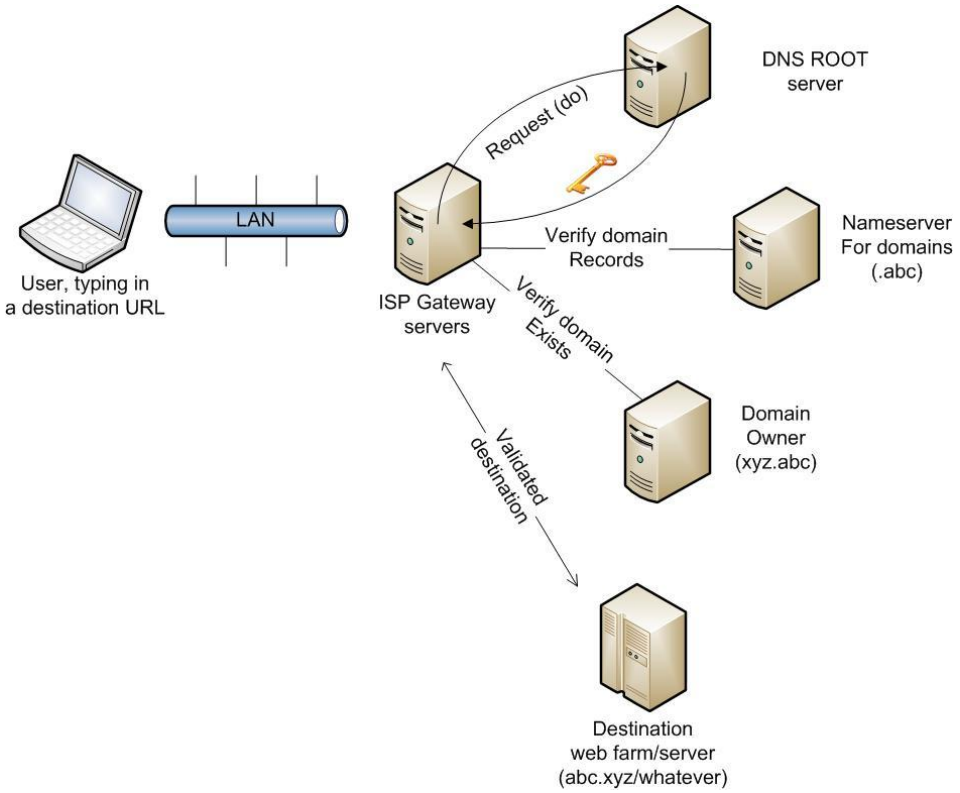
8.1.6 Cleanfeed

Cleanfeed is the name given to privately administered ISP level content filtering systems operating in the United Kingdom and Canada. Cleanfeed has been implemented in the UK by BT, Britain's largest Internet provider. This is a ISP based routers solution that redirects traffic that appear on Blacklists to special proxy servers.

8.1.7 DNSSEC

DNSSEC short for Domain Name System Security Extensions is an upgrade to the standard DNS (Domain Name System) designed to protect the internet from certain DNS based attacks. DNSSEC is in its early stages of being adopted.

DNSSEC provides a means to verify that the resulting IP address comes from a trusted source, solving the problem of a compromised DNS infrastructure returning incorrect IP address information for a domain name. DNSSEC does not address all DSN-related risks, such as, mistyping a domain name (e.g., movielabs.co instead of movielabs.com).



For DNSSEC to be most effective, broad adoption is necessary. The Internet community highly recommends DNSSEC adoption. EDUCAUSE provides resources to Higher Education institutions here: http://www.educause.edu/Resources/Browse/DNSSEC/34405

EDUCASE also provides information on DNS here: http://www.educause.edu/Resources/Browse/Domain%20Name%20System%20DNS/31429

Additional information about DNSSEC can be found here: http://dnssec.net and here: http://www.verisigninc.com/en_US/why-verisign/innovation-initiatives/dnssec/index.xhtml

DNSSEC is not the only initiative to improve the integrity of DNS. It is advisable to keep abreast of current developments, particularly at the EDUCASE resources referenced above.

DNSSEC is formally defined through a series of IETF RFCs: http://www.dnssec.net/rfc

8.1.8 BIND

BIND is the most widely deployed DNS software on the Internet. Notably, it has for a long time implemented site blocking capability. Other DNS server software includes Microsoft DNS[39], Dnsmasq[40]

BIND stands for Berkeley Internet Name Daemon as it was originally developed as at UC Berkeley. It is open source, deployed through the Internet Systems Consortium (ISC) at http://www.isc.org/software/bind

8.1.9 NAC

Network Access Control (**NAC**) is a client-side approach to computer network management (and security) that attempts to standardize the software in use (think mandatory Anti-Virus) as well as network policy enforcement as they attempt to access the managed network.

NAC is technical description term standardized by two industry bodies, the Trusted Computing Group and the IETF. Cisco is most well-known vendor with a NAC solution. Current NAC vendors include Enterasys, HP, Juniper (all members of the Trusted Computing Group and IETF). (Cisco is not a current member of the Trusted Computing Group.)

[39] http://en.wikipedia.org/wiki/Microsoft_DNS
[40] http://www.thekelleys.org.uk/dnsmasq/doc.html

9 APPENDIX E. REFERENCES AND RESOURCES

EDUCAUSE[41] is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

http://www-cdn.educause.edu/Resources/Browse/HEOA/34600

The Digital Citizen Project out of Illinois State University (ISU) has performed detailed research on campus behavior and surveyed technology for reducing file sharing: http://digitalcitizen.illinoisstate.edu/

10 ACKNOWLEGEMENTS

The authors gratefully acknowledge the contributions of Kent Wada who provided both technical expertise and wisdom regarding the practical application of technology in the campus environment.

[41] http://www.educause.edu/